UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PASSLOGIX, INC.,

Plaintiff,

- against -

2FA TECHNOLOGY, LLC, 2FA, INC., GREGORY SALYARDS, and SHAUN CUTTILL,

Defendants.

OPINION AND ORDER

08 Civ. 10986 (PKL)

APPEARANCES

PROSKAUER ROSE LLP
Steven M. Kayman, Esq.
Dan Goldberger, Esq.
1585 Broadway
New York, N.Y. 10036-8299

CADWALADER, WICKERSHAM & TAFT LLP
Hal S. Shaftel, Esq.
One World Financial Center
New York, N.Y. 10281

Attorneys for Plaintiff

LAURENCE SINGER, ATTORNEY-AT-LAW
Laurence Singer, Esq.
1629 K Street NW, Suite 300
Washington, D.C. 20006

Attorney for Defendants

Table of Contents

LEISURE, District Judge:

Plaintiff, Passlogix, Inc. ("Passlogix"), brings this fraud on the court allegation against defendants Gregory Salyards, 2FA Technology, LLC, and 2FA, Inc. for creating and sending an anonymous e-mail in an effort to expand discovery, cause Passlogix competitive harm, and garner a favorable settlement.

As a remedial measure, Passlogix asks the Court to dismiss 2FA's pleadings and award Passlogix costs and attorneys' fee. Passlogix also alleges that 2FA engaged in spoliation of evidence and asks for an adverse inference, preclusion, and costs. 2FA counter-alleges that Passlogix committed its own fraud on the court by bringing its erroneous fraud on the court allegation to delay adjudication on the merits.

The Court held a five-day evidentiary hearing on the issues of fraud on the court and spoliation of evidence and asked the parties to submit post-hearing memoranda. For the reasons set forth below, the Court holds that neither Passlogix nor 2FA has established by clear and convincing evidence that a fraud on the court was committed. The Court also holds that 2FA's failure to preserve certain documents led to the destruction of evidence in this case, requiring imposition of a $10,000 monetary fine.

BACKGROUND

Both Passlogix and 2FA Technology, LLC and 2FA, Inc. (collectively, "2FA") are in the business of developing and selling security-related software for managing access to restricted computerized systems. (Pl. Passlogix's Post-Hearing Mem. ("Mem.") 1.) The instant dispute arises out of Passlogix's lawsuit against 2FA, and 2FA's principals, Gregory Salyards ("Salyards") and Shaun Cuttill ("Cuttill"), for breach of a

licensing agreement in which 2FA purportedly agreed to develop identity-authentication software for Passlogix. Passlogix seeks (1) money damages against 2FA for breach of contract and tortious interference with business relations, and (2) a declaration that (a) it did not breach the licensing agreement or any other duties owed to 2FA or its employees, including Salyards and Cuttill, (b) 2FA has no valid grounds to terminate the licensing agreement and is obligated to continue abiding by the agreement, (c) Passlogix has not impermissibly used any confidential information or intellectual property of 2FA, and (d) Passlogix does not owe 2FA any money. (Am. Compl. ¶¶ 20-32.) In its Answer, 2FA asserts counterclaims against Passlogix for breach of contract, breach of the covenant of good faith and fair dealing, unfair competition, misappropriation of 2FA's intellectual property, and tortious interference with business relations. (Answer & Countercl. ¶¶ 32-46.)

In addition to the fraud on the court and spoliation allegations addressed in this decision, also pending before the Court is 2FA's motion to reverse Magistrate Judge Dolinger's denial of its motion to compel discovery and 2FA's motion for a preliminary injunction against Passlogix. These motions will be addressed in subsequent decisions.

I. Anonymous E-mails

The instant dispute was triggered by an anonymous e-mail sent on September 3, 2009, 4:00 p.m. Central Daylight Time ("CDT") from "passlogix-vgo-saw@hushmail.me" (the "September 3 e-mail"). The September 3 e-mail was sent to Passlogix's President and CEO, Marc Boroditsky, Passlogix's Chief Technology Officer, Marc Manza, two executives at a non-party business entity, Imprivata, Inc. ("Imprivata"), and Salyards and Cuttill.[1] (Passlogix Exhibit ("PX") 1.) The anonymous author, who purports to have "more than 15 years of development experience" and to have transitioned to Passlogix "earlier this year," asserts that Passlogix issued a "recent mandate to utilise Imprivat[a] and 2FA information that clearly oversteps . . . contractual and ethical obligations." (Id.) The anonymous author claims to be "appalled by the unprofessionalism and unethical behavior undertaken by the Passlogix engineering management organisation" and to "have been treated like a second-class citizen." (Id.) The September 3 e-mail also includes two attachments that contain specifications to Passlogix software under development. (See id.; (Evidentiary Hr'g Tr. ("Tr.") 44:23-45:5.) One attachment is titled "Master Func Spec v-GO SAW v1.5" and the other is titled "SAW Func Spec Iteration 2 v1.5." (PX 1; Tr. 45:3-5.)

[1] Cuttill never actually received the September 3 e-mail because his e-mail address was misspelled. (Evidentiary Hr'g Tr. ("Tr.") 532:3-11.)

Passlogix claims that the September 3 e-mail was not the first time that it received an anonymous e-mail from a hushmail.com e-mail address, and that on April 13, 2009, 3:59 p.m. CDT, Boroditsky and Mark Gillespie, a Passlogix employee, received an e-mail from "concernedatpasslogix@hushmail.com" (the "April 13 e-mail"). (PX 2.) The April 13 e-mail expresses concern about Passlogix losing "the Wal-Mart deal" and discloses Salyards' close relationship with "Adnan," a principal consultant at Deloitte & Touche who was brokering a deal with Wal-Mart for 2FA. (PX 2; Tr. 417:12-419:6, 542:15-20.) Cuttill testified that this e-mail was "detrimental to 2FA" because it "expose[d] a key relationship that [2FA] [was] pursuing to win the Wal-Mart deal," which "was the only way" for a small company like 2FA to get "in front of Wal-Mart," and "exposing that [relationship], in essence, killed [2FA's] opportunity at Wal-Mart." (Tr. 542:3-14.) In fact, Cuttill testified that after April 13, Adnan would not return Cuttill's e-mails. (Tr. 542:15-20.)

By letter dated September 14, 2009, counsel to 2FA wrote to Magistrate Judge Dolinger about the anonymous September 3 e-mail "because of the seriousness of the allegations set forth in the email, especially in light of 2FA's present Motion for Preliminary Injunction, filed on the basis of Passlogix's misappropriation of 2FA's intellectual property." (PX 30 at 2.)

In a separate letter dated October 27, 2009, Passlogix alleged that Salyards committed a fraud on the Court by authoring and transmitting the September 3 and April 13 e-mails. (PX 33.) Passlogix alleges that Salyards created and sent these e-mails to expand discovery, cause Passlogix competitive harm, and garner a favorable settlement—all of which constitute a fraud on this Court. (Mem. 6.)

II. Investigation Into Authorship of Anonymous E-mails

Within days of receiving the September 3 e-mail, Passlogix retained outside counsel to conduct an internal investigation into the sender of that e-mail and any evidence supporting the allegations set forth in that e-mail. (Tr. 24:25-25:12, 35:10-36:3; PX 34.) A report following the internal investigation concluded that the claims in the September 3 e-mail were false and that no individual at Passlogix identified any inappropriate request to utilize intellectual property from third parties. (PX 34 & 35; Tr. 36:17-22.)

In addition to its internal inquiry, Passlogix subpoenaed Hushmail.com ("Hush"), the Canadian e-mail service provider through which the September 3 and April 13 e-mails were sent. (Tr. 38:5-21.) Hush provided Passlogix with the Internet Protocol ("IP") address logs for the Hush accounts from which the anonymous e-mails were sent ("Hush logs"). (PX 48 & 49.)

"An IP address is a set of numbers . . . assigned to a computer in order for it to communicate on a network, which also includes communicating to the outside world; internet, web pages, e-mail as an example." (Tr. 146:20-23.) "An IP log is a log that many companies use to capture the source IP address of the network or computer that's connecting to the service . . . ." (Tr. 154:3-5.) The Hush logs reveal that both the September 3 and April 13 e-mails were sent from the IP address 70.114.246.62. (PX 48 & 49.) After the April 13 e-mail was sent, Hush captured additional log-ins from the IP addresses 70.114.246.202 and 64.186.161.2. (PX 49.) According to records that Passlogix obtained from Time Warner, the IP address 70.114.246.62 is registered to Salyards at 2FA's office location while the IP address 70.114.204.202 is registered to Salyards' wife, at their home address. (PX 40; Tr. 41:1-23, 156:9-20.) The final IP address—64.186.161.2—appears related to the Mark Hopkins Hotel in San Francisco, where Salyards and Cuttill were staying for a work conference from April 19 - April 24, 2009. (PX 37, 38, 49; Tr. 42:14-43:21.)

In addition to the Hush logs, Passlogix points to circumstantial evidence that Salyards authored both anonymous e-mails. Passlogix contends that the timing of each of the anonymous e-mails is suspect because the April 13 e-mail was sent during the course of a dispute regarding third party

discovery subpoenas and the September 3 e-mail was sent one day after Passlogix filed its brief in opposition to 2FA's motion for a preliminary injunction. (Def.'s Ex. ("DX") 1 (Passlogix Ltr. 11/6/09 at 1-2).) Additionally, Passlogix contends that because the September 3 e-mail was sent less than two weeks prior to the parties' settlement conference before Judge Dolinger, Salyards sent the e-mail to procure a more favorable settlement from Passlogix. (Mem. 6.) Salyards admits that he referenced the September 3 e-mail in settlement conversations with Boroditsky in the days following the September 3 e-mail. (See PX 29 ("We have a proposal for you that we feel best serves all concerned" (September 5, 2009); "Our attorney plans on raising the [September 3 e-mail] with the court this week, . . . I'm in NYC this weekend and would be willing to meet in the event you have a change of heart concerning our recent proposal" (September 12, 2009)); Tr. 338:20-339:13.) Passlogix further asserts that Salyards has admitted to receiving the confidential information attached to the September 3 e-mail from another anonymous e-mail purportedly sent to him from a Hush e-mail address in late June or early July 2009. (PX 33 at 4 n.1.) Also, Passlogix claims that Salyards may have received the attachments to the September 3 e-mail from a source within Passlogix. (DX 1 (Passlogix Ltr. 11/6/09 at 3).)

Cuttill testified about his own investigation into the origin of the anonymous e-mails. During the second or third week of September 2009, Cuttill and Salyards visited Hush "to find out what Hushmail was all about." (Tr. 576:22-577:16.) In late October or early November 2009—after Passlogix wrote this Court alleging that Salyards was the author of both anonymous e-mails—Cuttill interviewed 2FA employees that he thought would have had access to 2FA's computer network in April and September and checked all of 2FA's computers for evidence of the attachments to the September 3 e-mail, but found no evidence that anyone at 2FA sent the e-mails. (Tr. 572:16-575:5.) Cuttill did not take notes during his investigation, nor did he memorialize his findings in writing. (Tr. 573:15-16.)

III. Salyards' Defense and "IP Spoofing" Theory

Salyards testified under oath at his October 23, 2009 deposition and during the evidentiary hearing in January 2010 that he was not involved in the transmission of either e-mail. (Tr. 384:25-385:4.) He refutes Passlogix's claim that the confidential attachments to the September 3 e-mail were available to him or to 2FA. (DX 1 (2FA Ltr. 10/29/09 at 3-4 & 2FA Ltr. 11/9/09 at 3).) He also maintains that the mere content of the April 13 e-mail, which discloses a business opportunity with Wal-Mart that 2FA was pursuing as a competitor

to Passlogix, eliminates any motive that Salyards would have in sending that e-mail. (DX 1 (2FA Ltr. 10/29/09 at 2-3).) In arguing that no one at 2FA sent the September 3 e-mail, Salyards points to the use of the letter "s" in the spelling of words such as "organisation" and "utilise" in the e-mail, indicating British or Canadian authorship. (DX 1 (2FA Ltr. 11/9/09) at 3.)

Salyards notes that the IP address linked to the September 3 e-mail is not assigned to him specifically, but rather to 2FA's office location and is used by every computer sending e-mails from that location. (DX 1 (2FA Ltr. 10/29/09 at 2).) Moreover, Salyards contends that he was out with his family and friends at the time the September 3 e-mail was sent at 4:00 p.m. CDT,[2] and submitted affidavits from three individuals, two of whom specifically state that Salyards was with them from approximately 3:15 p.m. until 4:30 or 4:45 p.m. on September 3. (Id. at 4 & Ex. 2.) 2FA also notes that the anonymous e-mails are not evidence and, notwithstanding the fact that 2FA could have used the allegations in the September 3 e-mail in its reply brief in support of its motion for a preliminary injunction, it did not do so. (DX 1 (2FA Ltr. 11/9/09 at 2).)

Salyards proffers the affirmative defense of IP spoofing, stating that a Passlogix employee may have "spoofed" his IP

[2] There is no dispute that Cuttill was vacationing in Mexico when the September 3 e-mail was sent. (DX 1 (2FA Ltr. 10/29/09 at 4).)

address in an effort to impersonate him on the internet. (DX 1 (2FA Ltr. 10/29/09 at 1-2).) IP address spoofing is a practice whereby a person can make his true IP address appear to be any address he chooses. (Id. at 1.) 2FA asserts that IP spoofing can be accomplished from anywhere, as long as the impersonator knows a user's IP address. (Id. at 1; see also Tr. 391:22-25 (Salyards defining IP spoofing as "concealing your . . . IP address . . . and perpetrating to be something else when you're out on the Internet").) Salyards claims that, based on a decade of specialized training in computer security, including hacking and spoofing IP addresses to conduct "penetration testing" of security solutions, he knows how to conceal his IP address and that had he endeavored to create a fictitious e-mail, he would have ensured that it could not be traced back to him personally or to 2FA. (Tr. 389:3-11, 390:13-393:21; DX 1 (2FA Ltr. 10/29/09 at 2).)

IV. Chris Collier's Confession to Sending the April 13 E-mail and "Spoofing" Salyards' IP Address

Chris Collier, a former Passlogix employee who has over ten years of experience in the computer security industry, confessed under oath during a December 2, 2009 deposition that he wrote and sent the April 13 e-mail. (Collier Dep. 5:18-6:23, 8:11-14, 61:3-62:5.) Collier testified that he sent the April 13 e-mail

from his personal laptop computer while he was at 2FA's office without the knowledge of 2FA. (Collier Dep. 60:11-62:11, 76:15-19, 83:11-14.) Because he sent the April 13 e-mail from a wireless access point in 2FA's conference room, Collier did not need to spoof 2FA's IP address to make it appear that the e-mail was sent from 2FA. (Id. 62:4-8, 84:6-8.) After the initial e-mail was sent from 2FA's office, Collier said that he spoofed 2FA's IP address "[s]ix, maybe seven times" to check whether he received any responses to the April 13 e-mail from the e-mail recipients—Boroditsky or Gillespie. (Id. 86:2-4.) During his subsequent log-ins to Hush, Collier said that he concealed his IP address by substituting his IP address with "an IP address from the e-mail headers from Greg [Salyards]," by using software downloaded from the internet. (Id. 64:22-25, 70:12-21, 86:11-25.) When asked what program he used to spoof Salyards' IP address, Collier responded, "I can't be sure. Probably Mac IP Change, which is one that I've used many times before. That's the one I used." (Id. 86:23-25.) Collier also testified that the source of the content of the April 13 e-mail came from Cuttill, who disclosed to Collier 2FA's efforts to land the Wal-Mart deal during Collier's April 13 visit to 2FA's office. (Id. 108:15-110:15.) Collier no longer has the laptop that he used to send the April 13 e-mail because he "decommissioned" it and

gave it to a friend in need. (Id. 108:11-14; PX 45 at CC-000A ¶ 1.)

Cuttill corroborates Collier's account of visiting 2FA's office on April 13. Cuttill recalls being in the office on April 13 because he was preparing for a work conference ("RSA conference") in California the following week. (Tr. 532:14-533:8.) Cuttill states that Salyards was not in the office because he was watching his children that week since his wife was going to watch them the following week while Salyards was at the RSA conference. (Tr. 533:9-19.) Cuttill states that Collier arrived at 2FA's offices on April 13 "somewhere around 3:00, give or take maybe 15 minutes" to do work on "Oberthur cards." (Tr. 594:9-595:1; 585:13-19.) After Collier arrived, he and Cuttill "chatted for a little bit," "definitely less than ten minutes, probably less than five minutes," about the Wal-Mart deal. (Tr. 585:20-586:1. 594:12-25.) Then Cuttill set up Collier with internet in a conference room while Cuttill went to prepare for a 4 p.m. call. (Tr. 585:14-19; 595:1-11.) After Cuttill's 4 p.m. call was over, he and Collier worked on the Oberthur cards until 6 or 6:30 p.m. (Tr. 595:9-23.)

Collier testified that he did not send the September 3 e-mail. (Collier Dep. 65:8-17.) He did state, however, that in June 2009, he had a conversation with another Passlogix employee, Joseph Robinson, who expressed concerns similar to

those stated in the September 3 e-mail. (Id. 65:18-67:4, 77:17-78:24, 79:7-18.) Collier states that he suggested to Robinson to raise the issue with Boroditsky or, alternatively, send an e-mail through Hush since "[t]hey won't know who you are." (Id. 68:7-16, 98:19-99:21.) Collier says that he told Robinson that he used Salyards' IP address when he sent his own anonymous e-mail, though he did not tell Robinson what that IP address was. (Id. 98:14-18.) Salyards asserts that Robinson fits the profile of the author of the September 3 e-mail because Robinson lives in Canada, transitioned to Passlogix in April 2009 from a firm bought by Imprivata, the company mentioned in and copied on the September 3 e-mail, had fifteen years of technology experience, and was terminated by Passlogix in October 2009 for unexcused absences. (DX 19; Tr. 80:7-81:5; PX 53 at 2.)

Passlogix states that Collier's confession to sending the April 13 e-mail is unreliable since Collier admitted to lying about his role in the creation of the e-mail when Passlogix interviewed him as part of its internal investigation. (DX 4 at 2.) Passlogix underscores the secretive business ties Collier had with Salyards and Cuttill, evidenced by the fact that Collier testified that Cuttill provided him with the information used to write the April 13 e-mail. (Id.; Collier Dep. 53:21-54:2, 114:13-115:8, 118:13-19.) Passlogix also points to inaccuracies in Collier's testimony regarding when and where he

created the April 13 e-mail account, his Hush account password, and the extent of his communications with Salyards. (DX 4 at 2.) Collier testified that he set up the Hush account "a few days before the e-mail was sent." (Collier Dep. 84:10-12; 85:20-86:1.) However, the Hush logs indicate that the account was set up on April 13, 2009—the same day the e-mail was sent, just twenty-seven minutes before it was transmitted. (PX 49; PX 44 ¶ 6.) Collier also provided a password that he used for the Hush account, which Hush confirmed was inaccurate. (Collier Dep. 84:17-85:19; PX 41 & 44 ¶ 5.) Collier, however, noted that he could not "remember if that's exactly the password [he] used, because [he had not] been [on the website] for months now." (Collier Dep. 85:18-19.) Additionally, Collier testified that between April 13 and December 2, 2009, he spoke to Salyards "[p]robably 15 to 20 times," while phone records from October 2009 alone show that they spoke over thirty times. (Id. 118:13-15; PX 45.) With respect to the September 3 e-mail, Passlogix states that Collier's "suspicions" that Robinson sent that e-mail are inadmissible and unreliable. (Mem. 11.)

V. Expert Testimony Regarding IP Spoofing

The Court qualified Passlogix's expert in computer forensics and computer crime investigations, Andrew Obuchowski,

Jr., during a preliminary hearing on November 9, 2009,[3] based on Obuchowski's twelve years of law enforcement experience in computer crime forensics and three years of experience in private computer forensics, including "tracing of e-mails" and "analysis of how a computer was used . . . during the commission of an incident or crime." (Prelim. Hr'g Tr. 33:6-34:20, 36:11-37:7.) Obuchowski has taught computer crime investigations to law enforcement officers and is an adjunct professor at a criminal justice college in Massachusetts. (Id. 33:23-34:5.) Obuchowski has testified in several court proceedings "regarding computer crime and computer forensics," including IP spoofing. (Id. 34:6-35:10.)

Obuchowski concludes that spoofing a public IP address assigned by an Internet Service Provider,[4] such as Time Warner, "is not possible to the extent of being undetected" because "[t]he email message headers would show inconsistencies . . . [that] were not present in the email headers" from the April 13 and September 3 e-mails. (PX 36 ¶ 15; see also Tr. 153:9-13, 170:15-18.) Obuchowski also concludes that the MAC IP Change program that Collier claimed he used to spoof Salyards' IP

[3] At the end of the preliminary hearing, the Court permitted the parties to conduct additional discovery and reconvene for a more fulsome hearing where all relevant witnesses, particularly Salyards, could be present. (Prelim. Hr'g Tr. 61:22-67:9.)

[4] A private IP address is assigned to a user locally. When a user connects to the internet, the internet service provider (ISP)—Time Warner, in this case—assigns a public IP address. (Tr. 180:24-181:14.)

address "does not have the technical capability of changing an IP address that's assigned by Time Warner to make it appear that you are coming from 2FA's network unless you were actually on 2FA's network." (Tr. 164:6-19.) Obuchowski explains that the MAC IP Change Program only "changes [the] IP address of the computer that you install the software program on," and is not capable of "spoofing an Internet service provider." (Tr. 242:5-11.) Additionally, Obuchowski concludes that he is not "aware of" any "software on the market that can be used to spoof an Internet service provider" and that "any software program install[ed] on a local laptop computer . . . would not change the IP address assigned by an Internet service provider, in the example of Time Warner, that would reflect any change in the Hushmail logs." (Tr. 242:12-16, 623:17-624:2.) Obuchowski explains that, to access a website on the internet, two computers or networks must be able to communicate with each other. (Tr. 146:20-23.) They do so by sending information back and forth to each other's IP address (the same way a telephone number corresponds to a telephone, an IP address corresponds to a computer and/or network). (Tr. 146:20-147:3.) Thus, if someone tried to access Hush and conceal his own IP address by spoofing another IP address, Hush would respond by sending information to the computer/network associated with the "spoofed" IP address, not to the concealed IP address. (Mem.

10.) As a result, the spoofer would never be able to complete the process of logging into the Hush website or complete any other activity on the Hush website because he would not receive communication back from Hush, as it would instead be directed to the spoofed IP address. (Id.; see also Tr. 615:8-16.) Obuchowski acknowledges that if Collier sent the April 13 e-mail from 2FA's network, as Collier claims, "then 2FA's IP address would appear in the logs." (Tr. 231:22-25.) However, Obuchowski states that Collier did not send the April 13 e-mail because Collier was incorrect about when the April 13 Hush account was created and about the password he used to create it. (Tr. 165:4-166:25, 168:14-20; PX 41.)

Obuchowski created his own Hushmail test account during the course of his investigation, even though he did not mention the test account in either one of his declarations. (Tr. 234:10-24; PX 36 & 40.) Obuchowski "walk[ed] through the same steps in creating an e-mail account as Mr. Collier claimed that he did" and sent a test e-mail to his work e-mail address. (Tr. 235:1-6.) Obuchowski only used the test account once to see what services Hush offers and what the e-mail headers look like when a Hush e-mail is received. (Tr. 235:12-19.) Obuchowski stated that the test e-mail he sent appeared just like the other e-mails sent from the April 13 and September 3 e-mail addresses, although he did not have a copy of, or a log from, the test e-

mail. (Tr. 235:5-23.) When asked for his password to the Hush account at the evidentiary hearing on January 14, 2010, Obuchowski could not recall; nor could he recall the date that he created the account, but noted that it would have been before his first declaration, which was dated November 6, 2009. (Tr. 235:24-236:5.)

2FA does not proffer a computer forensics expert in rebuttal; instead, it relies on Salyards' and Cuttill's personal experiences to challenge Obuchowski's conclusion about the unfeasibility of IP spoofing. Salyards testified that he has twelve years of experience in computer forensics and computer security, including hacking and spoofing, and has spoofed IP addresses to conduct "penetration testing" of security solutions as part of his work and that he knows how to conceal his IP address. (Tr. 388:19-389:11, 390:13-392:18.) Cuttill, 2FA's Chief Technology Officer, has fourteen years of experience in strong authentication computer software. (Tr. 519:19-521:9.) Cuttill testified that he has spoofed IP addresses by concealing his own IP address and selecting an IP address that belonged to a company's internal network. (Tr. 565:9-567:17.) Cuttill also said that, contrary to Obuchowski's conclusions, he has spoofed a public IP address that has been assigned by an Internet Service Provider, such as Time Warner, as part of security analysis projects. (Tr. 589:25-591:20.) He said he typically

spoofs "by hand" but has used software that helps with encryption matters. (Tr. 591:5-9.) Although he has never used the MAC IP Change program to spoof an IP address, Cuttill noted that there are "a number of programs that are called very similar to that." (Tr. 591:21-592:11.)

Cuttill and Salyards also contend that the Hush logs exonerate Salyards because the Mark Hopkins Hotel, where they stayed from April 19 to April 24, 2009, never assigned Salyards an IP address ending in ".2"—the IP address that the Hush logs captured. (Def.'s Opp'n to Pl. Passlogix's Post-Hearing Mem. ("Opp'n Mem.") 18.) The Hush logs captured two log-ins to Hush from the IP address 64.186.161.2—the first on April 20 at 10:30 a.m. Pacific Daylight Time ("PDT") and the second on April 23 at 10:15 p.m. PDT. (PX 49 (emphasis added).) The Mark Hopkins Hotel records indicate that Salyards purchased a higher level of service ($15.95) at the time of the first log in. (PX 49 at IHG 3.) This higher level of service, which was purchased from Salyards' computer (MAC Address 00:21:70:A9:54:51),[5] assigned Salyards' computer an IP address of 64.186.161.12. (PX 38 at IHG 3 (emphasis added).) Also during the time of the first log-in, another room at the Mark Hopkins Hotel—which Salyards paid for—used a computer with a different MAC Address

[5] A MAC address is a physical address associated with a computer's unique network adaptor. (Tr. 193:9-10.)

(00:21:9B:E1:BD:5F) to purchase a lower level of internet service ($12.95) that did not assign a specific IP address. (PX 38 at IHG 7.) The second log-in on April 23, 2009, 10:15 p.m. PDT, occurred when a lower level of service ($12.95) was purchased through Salyards' computer (MAC Address 00:21:70:A9:54:51). (See PX 38 at IHG 4.)

Obuchowksi acknowledges that the IP address 64.186.161.12, which was assigned to Salyards when he purchased a higher level of internet service at the Mark Hopkins Hotel, is not reflected in the Hush logs. (Tr. 191:1-15.) He reconciles this discrepancy by explaining that, when a lower level of service is purchased, the Mark Hopkins Hotel assigns its own IP address through a public IP service; therefore, the .2 IP address reflected in the Hush logs must have been the public IP address that the Hotel assigned when the lower level of service was purchased by the non-Salyards MAC address on April 20 and by the Salyards MAC address on April 23. (Tr. 191:9-22, 240:17-241:16.)

VI. Evidentiary Hearing in January 2010

The Court held an evidentiary hearing on January 13, 2010, intended to last no more than a day and a half, but which went on for five days. At the hearing, Passlogix proffered two arguments: (1) the Hush logs, Mark Hopkins Hotel records, and

other circumstantial evidence establish that Salyards committed a fraud on the court by (a) transmitting the September 3 e-mail to procure a better settlement from Passlogix and cause Passlogix commercial harm, (b) transmitting the April 13 e-mail as pretext to obtain third party discovery, and (c) orchestrating Collier's confession to writing the April 13 e-mail; and (2) 2FA engaged in spoliation of evidence by failing to implement a litigation hold policy at the onset of this litigation, leading to the destruction of relevant documents. (Tr. 8:4-12:1.) In support of its position, Passlogix presented live testimony from Boroditsky, Manza, Scott Bonnell, and Salyards. It also presented live expert testimony from Obuchowski and Doug Brush, who the Court qualified on a limited basis as an expert in computer forensics. (Tr. 481:8-482:1.) As a remedy for Salyards' alleged fraud on the court, Passlogix asks the Court to dismiss 2FA's pleadings and award Passlogix costs for its investigation into the authorship of the e-mails. (Mem. 35.) Passlogix also requests an adverse inference, preclusion, and costs for 2FA's alleged spoliation of evidence. (Id. 33-34.)

2FA asserts the following claims and affirmative defenses: (1) Collier's admission to writing the April 13 e-mail and spoofing Salyards' IP address subsequent to sending that e-mail vindicates Salyards; (2) there is circumstantial evidence

pointing to Robinson as the author of the September 3 e-mail; (3) Passlogix, not 2FA, committed a fraud on the court by submitting both anonymous e-mails to the Court with a bad faith intent to delay adjudication on the merits; and (4) no spoliation of evidence occurred because the documents that Salyards did not preserve were not evidence when they were deleted and, even if they were evidence, they would have been helpful to 2FA, not Passlogix. (Opp'n Mem. 1, 5, 8, 29.) 2FA presented live testimony from Cuttill and Boroditsky, in addition to Dr. Alan Perlman, from whom the Court heard testimony but declined to qualify as an expert in linguistics. (Tr. 259:14-260:5, 261:1-8.) 2FA asks the Court to dismiss Passlogix's claims with prejudice and award 2FA relief, including but not limited to reimbursement for the costs incurred to defend itself and Salyards, which, as of January 21, 2010, totaled approximately $200,000. (Opp'n Mem. 35; Tr. 569:10-18.)

DISCUSSION

The Court first addresses whether either party has established that its adversary committed a fraud on the court. Then the Court turns to Passlogix's allegation that 2FA engaged in the spoliation of evidence.

I. Fraud on the Court

Passlogix fails to establish that Salyards committed a fraud on the court. Likewise, 2FA fails to establish that Passlogix committed a fraud on the court and, therefore, is not entitled to amend its counterclaims to assert a malicious prosecution claim against Passlogix. In reaching these conclusions, the Court first addresses the legal standard for fraud on the court. Then the Court explains why each party has failed to demonstrate that its adversary committed a fraud on the Court.

A. Legal Standard

A fraud on the court occurs where it is established by clear and convincing evidence "that a party has sentiently set in motion some unconscionable scheme calculated to interfere with the judicial system's ability impartially to adjudicate a matter by . . . unfairly hampering the presentation of the opposing party's claim or defense." McMunn v. Mem'l Sloan-Kettering Cancer Ctr., 191 F. Supp. 2d 440, 445 (S.D.N.Y. 2002) (quoting Aoude v. Mobil Oil Corp., 892 F.2d 1115, 1118 (1st Cir. 1989)); see also Hargrove v. Riley, No. 04 Civ. 4587, 2007 U.S. Dist. LEXIS 6899, at *36 (E.D.N.Y. Jan. 31, 2007); Shangold v. Walt Disney Co., No. 03 Civ. 9522, 2006 WL 71672, at *4 (S.D.N.Y. Jan. 12, 2006); Intelli-Check, Inc. v. Tricom Card

Techs., Inc., No. 03 Civ. 3706, 2005 WL 3533153, at *11 (E.D.N.Y. Dec. 22, 2005); Scholastic, Inc. v. Stouffer, 221 F. Supp. 2d 425, 439 (S.D.N.Y. 2002). The essence of fraud on the court is "when a party lies to the court and his adversary intentionally, repeatedly, and about issues that are central to the truth-finding process." McMunn, 191 F. Supp. 2d at 445. Fraud on the court, therefore, does not merely "embrace any conduct of an adverse party of which the court disapproves;" rather, it "embrace[s] only that species of fraud which does or attempts to, defile the court itself." Kupferman v. Consol. Research & Mfg. Corp., 459 F.2d 1072, 1078 (2d Cir. 1972) (Friendly, C.J.) (citation and internal quotation marks omitted) (discussing fraud on the court in the context of a Rule 60(b) motion). Consequently, "an isolated instance of perjury, standing along, will not constitute a fraud upon the court." McMunn, 191 F. Supp. 2d at 445; see also Jung v. Neschis, No. 01 Civ. 6993, 2009 WL 762835, at *21 (S.D.N.Y. Mar. 23, 2009); Skywark v. Isaacson, No. 96 Civ. 2815, 1999 WL 1489038, at *14 (S.D.N.Y. Oct. 14, 1999). "Rather, fraud upon the court 'occurs where a party has acted knowingly in an attempt to hinder the fact finder's fair adjudication of the case and his adversary's defense of the action.'" McMunn, 191 F. Supp. 2d at 445 (quoting Skywark, 1999 WL 1489038, at *14).

The Court has inherent authority "to conduct an independent investigation in order to determine whether it has been the victim of fraud." Chambers v. NASCO, Inc., 501 U.S. 32, 44, 111 S. Ct. 2123, 115 L. Ed. 2d 27 (1991); see also Universal Oil Prods. Co. v. Root Ref. Co., 328 U.S. 575, 580, 66 S. Ct. 1176, 90 L. Ed. 1447 (1946). "Because of their very potency, inherent powers must be exercised with restraint and discretion." Chambers, 501 U.S. at 44. The Court's inherent powers serve "to do whatever is reasonably necessary to deter abuse of the judicial process and assure a level playing field for all litigants." Shangold, 2006 WL 71672, at *4.

If it is shown by clear and convincing evidence that a party perpetrated a fraud on the Court, the Court may consider the following five factors in determining an appropriate sanction: (i) whether the misconduct was the product of intentional bad faith; (ii) whether and to what extent the misconduct prejudiced the injured party; (iii) whether there is a pattern of misbehavior rather than an isolated instance; (iv) whether and when the misconduct was corrected; and (v) whether further misconduct is likely to occur in the future. See Shangold, 2006 WL 71672, at *4; Intelli-Check, 2005 WL 3533153, at *11; Scholastic, 221 F. Supp. 2d at 444; McMunn, 191 F. Supp. 2d at 461. When faced with a fraud on the court, "[t]he available sanctions at a court's disposal . . . range from the

issuance of a jury charge on falsehoods under oath, to the imposition of attorney's fees occasioned by the conduct in question, and finally to the entry of judgment against the offending party." Skywark, 1999 WL 1489038, at *14 (internal citations omitted).

B. Application

First, the Court explains the showing required to establish a fraud on the court claim. Next, the Court applies the fraud on the court standard in holding that neither Passlogix nor 2FA has demonstrated that its adversary committed a fraud on the court by its conduct in this litigation.

1. 2FA Misstates the Fraud on the Court Standard

2FA insists that "[i]t is essential - it is the foundation of fraud on the court - that the party accused first submits evidence, evidence that eventually is found to be fraudulent or fabricated. Otherwise there cannot possibly be fraud on the Court." (Opp'n Mem. 4.) 2FA argues that although it wrote a letter to Magistrate Judge Dolinger dated September 14, 2009, bringing the anonymous misappropriation claims in the September 3 e-mail to Judge Dolinger's attention, it never attached the September 3 e-mail and, thus, did not "submit" evidence. (Id.) Instead, 2FA states that it was Passlogix that "submitted" both

anonymous e-mails by attaching them as exhibits to Passlogix's October 27, 2009 letter to this Court. (Id. 1.) Moreover, 2FA asserts that neither anonymous e-mail constitutes "evidence" under the Federal Rules of Evidence. (Id. 4.) Since Passlogix cannot make this threshold showing, 2FA insists that Passlogix's fraud on the court allegation fails as a matter of law. (Id.)

2FA misinterprets the requirements necessary to establish a fraud on the court. 2FA provides the holdings of five fraud on the court cases, which, as 2FA states correctly, sanctioned parties for "submitting" actual "evidence" to the court. See Hargrove, 2007 U.S. Dist. LEXIS 6899, at *11, *38 (dismissing plaintiff's claims with prejudice where plaintiff provided fraudulent documents to defendants during discovery and attached said documents as exhibits to his complaint and his affidavit in opposition to defendant's motion for summary judgment); Shangold, 2006 WL 71672, at *5 (dismissing plaintiff's misappropriation case with prejudice and awarding costs and attorneys' fees to defendants where plaintiffs "fabricated evidence and manipulated the judicial process"); Scholastic, 221 F. Supp. 2d at 444 (granting plaintiff's motion for sanctions where defendant "perpetuated a fraud on the Court through her submission of fraudulent documents [as exhibits to her counterclaims] as well as her untruthful testimony"); McMunn, 191 F. Supp. 2d at 452, 454, 462 (dismissing plaintiff's action

with prejudice and awarding monetary sanctions where plaintiff perpetuated a fraud on the court by tampering with evidence and repeatedly providing false testimony); Cerruti 1881 S.A. v. Cerruti, Inc., 169 F.R.D. 573, 574 (S.D.N.Y. 1996) (granting plaintiffs' motion to strike defendants' answer and all but one counterclaim and awarding plaintiffs costs and attorneys' fees where defendants, through their principal, fabricated evidence and offered false testimony). As these cases demonstrate, submitting false evidence to a court may rise to the level of a fraud on the court; however, it is not the only way to commit a fraud on the court. A fraud on the court occurs where a party: (1) "improperly influence[es] the trier," McMunn, 191 F. Supp. 2d at 445 (citation and internal quotation marks omitted); (2) "unfairly hamper[s] the presentation of the opposing party's claim or defense," Id. (citation and internal quotation marks omitted); (3) "lies to the court and his adversary intentionally, repeatedly, and about issues that are central to the truth-finding process," Id.; or (4) "knowingly submit[s] fraudulent documents to the Court," Scholastic, 221 F. Supp. 2d at 443.

Given this clarification, the Court holds that even if the anonymous e-mails are not "evidence" under the Federal Rules of Evidence and 2FA did not "submit" the e-mails to the Court, these two facts do not obviate the need for the Court to

determine whether 2FA engaged in an "unconscionable scheme" to interfere with the adjudication of this case by unfairly hampering Passlogix's claims or defenses or by lying to the court and Passlogix about issues central to the case. See Hargrove, 2007 U.S. Dist. LEXIS 6899, at *36; Scholastic, 221 F. Supp. 2d at 439; McMunn, 191 F. Supp. 2d at 445; Skywark, 1999 WL 1489038, at *14. Below, the Court analyzes whether a fraud on the court has been established.

2. Passlogix has Failed to Establish that Salyards Committed a Fraud on the Court

Passlogix has failed to present clear and convincing evidence that Salyards authored the April 13 and September 3 e-mails and used them to commit a fraud on the Court. Below, the Court first addresses the testimony offered by Passlogix's expert, Obuchowski, and determines to what extent to credit his conclusions. Then, the Court analyzes the evidence that Passlogix submits in support of its claim, and explains why, in totality, the evidence does not meet Passlogix's burden of proof.

a. Expert Testimony by Obuchowksi

"[A]n expert testifying on the basis of experience may form his conclusions by applying his extensive experience to the

facts of the case." In re Methyl Tertiary Butyl Ether Prods. Liab. Litig., No. M21-88, 2008 WL 1971538, at *10 (S.D.N.Y. May 7, 2008); see also Kumho Tire Co., Ltd. v. Carmichael, 526 U.S. 137, 152, 119 S. Ct. 1167, 143 L. Ed. 2d 238 (1999). Where, as here, an expert's "qualifications and testimony rest on his . . . experience and not on scientific, mathematical or social science studies or calculations, . . . [the expert] must . . . apply his experience to the facts using the same intellectual rigor a professional [in his field] would use in practice." In re Methyl, 2008 WL 1971538, at *10; see also Kumho, 526 U.S. at 152 ("[A]n expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field."). Contentions that the expert's "'assumptions are unfounded go to the weight, not the admissibility, of the testimony.'" In re Methyl, 2008 WL 1971538, at *12 (quoting Boucher v. U.S. Suzuki Motor Corp., 73 F.3d 18, 21 (2d Cir. 1996)); see also McCullock v. H.B. Fuller Co., 61 F.3d 1038, 1044 (2d Cir. 1995) (McLaughlin, J.) (stating, with respect to a scientific expert, that "[d]isputes as to the strength of [the expert's] credentials, faults in his use of . . . [a particular] methodology, or lack of textual authority for his opinion, go to the weight, not the admissibility, of his testimony").

Where, as here, the Court acts as the trier of fact, it uses "the discretion given to it . . . [to] parse and evaluate the evidence . . . for its weight and worth." United States v. Alcan Aluminum Corp., No. 03 Civ. 0765, 2006 U.S. Dist. LEXIS 39042, at *4 (N.D.N.Y. June 9, 2006); see also New York v. Solvent Chem. Co., Inc., No. 83 Civ. 1401C, 2006 U.S. Dist. LEXIS 65595, at *4 (W.D.N.Y. Sept. 14, 2006) ("[T]he concerns expressed in Daubert and Kumho Tire about the need for the trial court to guard against the admission of unreliable scientific or technical evidence are not implicated in a non-jury trial."). Pursuant to its role as factfinder, the Court may credit an expert's testimony in whole or in part, regardless of whether another expert is called in rebuttal. See Giles v. Rhodes, 171 F. Supp. 2d 220, 226, 230 (S.D.N.Y. 2001) (denying plaintiff's motion for a new trial where jury had the power to refuse to credit plaintiff's expert's opinion, even though another expert was not called to rebut it); accord Leonard B. Sand, et al., 4 Modern Federal Jury Instructions-Civil ¶ 76-9 cmt. ("[E]xpert testimony is designed to assist the jury to reach an independent decision on the facts, and . . . is not a substitute for the jury's common sense evaluation of the evidence." (emphasis in original)).

While the Court credits much of Obuchowski's expert testimony, it declines to credit some of his ultimate

conclusions. The Court credits Obuchowksi's conclusions that, in his experience, (1) he has not come across software capable of doing the kind of IP spoofing that is alleged here, and (2) the MAC IP Change Program is incapable of doing the kind of IP spoofing that is alleged here. However, the Court declines to credit Obuchowski's broader conclusion that spoofing an IP address assigned by an internet service provider ("ISP")—the type of spoofing that is alleged to have been done here—is technologically impossible. (See Passlogix's Post-Hearing Reply Mem. ("Reply Mem.") 4 ("Obuchowski's conclusions are unrebutted that . . . IP address spoofing is not technologically feasible here . . . ." (emphasis in original)).) This conclusion is contradicted by Obuchowski's initial declaration, which states that "spoof[ing] the IP address in order for it to appear as 70.114.246.62 is extremely difficult and highly improbable," rather than impossible. (PX 36 ¶ 14.) Similarly, at the preliminary hearing, Obuchowski equivocated about whether it is possible to spoof an IP address assigned by an ISP. (See Prelim. Hr'g Tr. 39:13-17 ("[B]ecause an IP address is already assigned by an Internet service provider to a company or to an individual, . . . it's very difficult, if at all, to spoof that because that IP address is assigned." (emphasis added)).) Obuchowski's more nuanced conclusion that "IP spoofing of an [ISP] IP address is not possible to the extent of being

undetected" also is problematic because Obuchowski does not explain what kind of "inconsistencies" would appear in the "email message headers." (PX 36 ¶ 15 (emphasis added).) Obuchowski states that "jumps" in the e-mail headers are "one attribute" that "would lead [one] to believe that . . . potential IP spoofing existed"; however, he does not explain what a "jump" might look like in the e-mail headers here or whether there are other indicia of spoofing that he considered and concluded did not exist in the e-mail headers. (Prelim. Hr'g Tr. 40:12-14.) Also, there is personal experience testimony contradicting Obuchowski's conclusion that spoofing an IP address assigned by an ISP is technologically impossible, albeit by interested lay parties. Both Salyards and Cuttill testified to having spoofed IP addresses in their personal experience and Cuttill specifically testified to spoofing a public IP address assigned by an ISP. (Tr. 389:3-11, 390:13-392:3, 565:9-567:17, 589:25-591:25.)

The Court also finds Obuchowski's conclusions regarding how the Mark Hopkins Hotel assigns and routes IP addresses inconclusive at best, as Obuchowski admits that his conclusions are not based on personal knowledge about the Hotel's IP address routing practices. (See Tr. 213:20-21 ("How the hotel is assigning [its] IP addresses and their uses that they use them for, I do not know."), 618:5-11 (stating that "Mark Hopkins did

not supply information in the records" regarding its IP address routing practices and that he is "not sure exactly how Mark Hopkins is routing traffic").)

While the Court does not form its own judgment regarding whether spoofing an IP address assigned by an ISP is technologically feasible, it holds that Obuchowki's equivocating statements and inconsistencies noted elsewhere in this decision lead the Court to decline to credit his conclusion that such spoofing is impossible.

b. April 13 E-mail

The substance of the April 13 e-mail primarily relates to Wal-Mart, a Passlogix customer with whom Passlogix was finalizing an agreement. (PX 2; Mem. 16.) The e-mail also references Oracle, as well as an executive, Adnan, from Deloitte & Touche—all companies that 2FA was seeking to subpoena in connection with the underlying litigation. (PX 2; Mem. 16.) The anonymous author of the April 13 e-mail claims that Passlogix is in jeopardy of losing the Wal-Mart account because a certain Passlogix executive was leaking Passlogix's information. (PX 2.) The e-mail also references 2FA and claims that Adnan "has a lot of respect for [Salyards]" and states that "[h]opefully Passlogix's legal issues will not spill over to [the Wal-Mart] account." (Id.) Passlogix considered the April

13 e-mail when investigating the September 3 e-mail because the April 13 e-mail is "the only other anonymous, Hush email that Passlogix management has ever received." (Mem. 3.) Passlogix's stated purpose in introducing the April 13 e-mail "is to reveal a pattern of misconduct, and thereby corroborate Salyards' culpability for the critical September 3 Email." (Id. 15.)

i. Evidence Presented by Passlogix

Passlogix's strongest evidence that Salyards authored the April 13 e-mail are the logs that Passlogix subpoenaed from Hush, which indicate that the April 13 e-mail was sent from 2FA's office IP address. (See PX 49.) Passlogix contends that "the April 13 Hush Log reflects IP addresses that notably shift from Salyards' office to his home in Austin; from Austin to a specific San Francisco hotel, where he stayed while attending a conference; and then back to Austin." (Mem. 17.) Passlogix notes that each log-in to Hush syncs "precisely to Salyards' moving whereabouts": from work (April 13, 6:15 p.m. CDT), to home (April 13, 10:38 p.m. CDT), to work (April 14, 3:19 p.m. CDT), to work again (April 15, 8:58 p.m. CDT), to work again (April 16, 10:29 a.m. CDT), to work again (April 17, 10:31 a.m. CDT), to San Francisco (April 20, 10:30 a.m. PDT), to San Francisco again (April 23, 10:15 p.m. PDT), and back to work (April 27, 1:26 p.m. CDT). (Mem. 17-18; PX 49.) Passlogix

insists that "the likelihood that a spoofer would be able to accurately capture the[se] different IP addresses . . . is not credible." (Mem. 18.)

Passlogix points to timing and motive for corroboration, stating that Salyards sent the April 13 e-mail to Boroditsky and Gillespie to gain leverage in a discovery dispute in which 2FA sought to serve third-party subpoenas on business entities with whom Passlogix has commercial relationships. (See Mem. 15-16.) Passlogix contends that the unrebutted testimony of its expert, Obuchowski, confirms that the Hush logs and the records from the Mark Hopkins Hotel provide dispositive evidence that Salyards authored the April 13 e-mail. (See Mem. 2-3; PX 36, 38, & 44; Tr. 153:9-13.)

Passlogix also presents evidence contradicting Collier's confession to sending the April 13 e-mail. Obuchowski states that Collier did not send the April 13 e-mail because Collier was incorrect about when the April 13 Hush account was created and about the password he used to create it. (Tr. 165:4-166:25, 168:14-20; PX 41.) Obuchowski also states that the MAC IP Change program that Collier recalled using to conceal his IP address "does not have that capability." (Tr. 164:7-11.) Moreover, Obuchowski concludes "that there is no evidence of IP spoofing as being claimed" because the spoofing that 2FA alleges

would have left evidence in the header of the April 13 e-mail, which is not present. (Tr. 153:9-13, 170:15-18; PX 36 ¶ 15.)

To further discredit Collier's admission, Passlogix points to Collier's activities during the time period when the April 13 e-mail was sent. First, Doug Brush, who the Court qualified on a limited basis as an expert in computer forensics (Tr. 481:8-482-1), testified that on April 13, 2009, between 3:25 p.m. and 4:55 p.m. CDT, when Collier claims to have been at 2FA's office, there is evidence of computer user activity on Collier's work laptop under his username, including a printer installation. (Tr. 482:17-21; PX 55.) Brush also found evidence of web browsing on Collier's work laptop during this time period. (Tr. 483:19-484:4.) Second, Passlogix contends that Collier was e-mailing a Passlogix employee, Jennifer Kilmer, through his Passlogix e-mail account during the time that he claims to have been at 2FA's office. (Tr. 49:16-51:11; PX 56.) Third, Passlogix argues that Collier's phone records indicate that Collier was on a thirteen-minute phone call with Salyards on April 13 between 3:02 and 3:15 p.m. CDT, which contradicts Cuttill's testimony that Collier arrived at 2FA's office around 3:00 p.m. and that the two spoke for "about ten minutes or less." (Tr. 594:9-25; PX 45 at CC10, Item 212.) Fourth, Passlogix argues that Collier would not have had enough time to set up the Hush account and send the e-mail because Collier was

on a sixteen-minute phone call with a Passlogix employee, Stephan Wardell, during the time frame that the Hush account was being set up. (Tr. 167:1-168:13; PX 45 at CC10, Item 213.)

ii. Evidence Rebutted by 2FA

2FA rebuts Passlogix's evidence that Salyards authored the April 13 e-mail. First, 2FA maintains that the mere content of the April 13 e-mail, which discloses a business opportunity with Wal-Mart that 2FA was pursuing as a competitor to Passlogix, eliminates the possibility that Salyards—the President, CEO, and co-founder of 2FA—would have sent it to Passlogix. (Opp'n Mem. 9; Tr. 385:22-25.)

Second, 2FA contends that Collier's sworn confession to writing the April 13 e-mail discredits any suggestion that Salyards authored it. (Opp'n Mem. 9.) Collier's motive for sending the April 13 e-mail supports this conclusion. Collier testified—and Cuttill confirmed—that he learned about 2FA competing for the Wal-Mart opportunity from Cuttill during a visit to 2FA's office. (Collier Dep. 108:15-110:15; Tr. 536:22-537:16.) Collier explained that, prior to his employment at Passlogix, he "spent and invested a lot of time and energy into the Wal-Mart account" and felt that the "deal was extremely important to the success of Passlogix," especially after just transitioning from a company that went out of business, so he

sent the e-mail to "warn[] Passlogix about threats at Wal-Mart." (Collier Dep. 61:15-16, 76:20-77:13).

Third, 2FA refutes Obuchowski's conclusions regarding the implausibility of IP spoofing. Collier testified that he is familiar with Hush and IP spoofing. (See Collier Dep. 107:8-14 (stating that although he had "not used Hush in years" prior to sending the April 13 e-mail, he has used Hush "three or four times before . . . to send secure e-mail.").) Collier explained that he was aware that Hush tracks the IP addresses that interact with it

> [b]ecause it's kind of the second half of the equation. . . . [A]nyone in the security industry I hope would know that . . . an anonymous e-mail service with the big disclaimer that says it at the bottom of their home page before you log on, you have to know that you're not truly anonymous unless you change that [IP] address.

(Id. 107:22-108:10.) Collier testified that he did not spoof 2FA's IP address when he sent the April 13 e-mail since he sent the e-mail from 2FA's office network. (Collier Dep. 62:4-11, 76:15-19, 83:11-14, 84:6-8.) Obuchowski acknowledges that if Collier sent the April 13 e-mail from 2FA's network, "then 2FA's IP address would appear in the logs." (Tr. 231:22-25.) To explain why the Hush logs appear to track Salyards' movement from work, to home, to the Mark Hopkins Hotel, 2FA points to Collier's testimony, which explains that in signing on to Hush

following the April 13 e-mail, Collier used an IP address "from the e-mail header properties of an e-mail that [he] had from 2FA." (Collier Dep. 87:16-18, 70:12-21.) When asked whether he used the same IP address every time he logged on to Hush, Collier responded that he "was less interested in the exact numbers than . . . that it came from the same source, which would have been, unfortunately, Greg Salyards[] at the time." (Id. 87:21-88:1.) Collier then reiterated that he used "the same IP address or range of IP addresses based upon a 2FA e-mail." (Id. 88:18-89:1.) Collier's only stated reason for using Salyards' IP address was that he sent the April 13 e-mail from 2FA's "IP address the first time and just to maintain . . . the same thing. It wasn't relevant. It didn't seem relevant." (Id. 88:2-12.) Cuttill also suggests that Collier may have had a typo when spoofing Salyards' Mark Hopkins Hotel IP address ending in .12, resulting in the .2 IP address logged by Hush. (Tr. 602:16-603:2.) Moreover, Salyards challenges Passlogix's assertion that the Hush logs track his "exact geographical location," (Mem. 18), since Passlogix has not introduced evidence that Salyards actually was at home or at his office during the times captured by Hush. For instance, the Hush log from April 15, 8:58 p.m. CDT indicates that the account was accessed from Salyards' work IP address at a time when, if

compared to the other work entries captured by Hush, Salyards would have been at home. (PX 49.)

With respect to the gaps in Collier's testimony, 2FA contends that Collier said that he did not remember if the Hush password he provided Passlogix was "exactly the password [he] used, because [he had not] been there for months now." (Collier Dep. 85:18-19.) Collier also said that he "can't be sure" that the MAC IP Change program was indeed the program he used to spoof Salyards' IP address to log on to Hush after April 13. (Id. 86:23-25.) Collier does not have the laptop that he used to send the April 13 e-mail to corroborate his sending of the e-mail because he "decommissioned" it and gave it "to a friend in need." (PX 45 at CC-000A; see also Collier Dep. 108:11-14.)

Fourth, 2FA insists that the Mark Hopkins Hotel records exonerate Salyards since they show a different IP address than the one indicated on the Hush logs. (Opp'n Mem. 18.) Specifically, the Mark Hopkins Hotel records indicate that, over the course of Salyards' five-night stay, two levels of internet services were purchased for the rooms Salyards paid for: a higher level, which assigned the guest a specific IP address, and a lower level, which did not assign a specific IP address. (PX 38.) When the higher level of service was purchased from April 20 - April 23, 2009, the rooms that Salyards paid for were assigned two IP addresses: 64.186.161.12 and 64.186.161.57.

(Id.) The Hush logs, however, document two log-ins to Hush from a slightly different IP address—64.186.161.2—on (1) April 20, 10:30 a.m. PDT, and (2) April 23, 10:15 p.m. PDT. (PX 49.) 2FA claims that the Hush logs exonerate Salyards because the Mark Hopkins Hotel never assigned Salyards an IP address ending in ".2"—the IP address the Hush logs captured. (Opp'n Mem. 18.)

Obuchowski attempts to reconcile this inconsistency by insisting that "[t]he IP address of .2 and .12 both resolve back to the Mark Hopkins Hotel." (Tr. 213:9-10.) Obuchowski states that it is common for hotels to have multiple IP addresses "facing the Internet," such that when a guest purchases a lower level of internet service that does not assign a particular IP address, the guest is routed to one of the hotel's available IP addresses—in this case, the .2 IP address that Hush captured. (Tr. 191:9-22, 240:17-241:16, 614:3-15.) Obuchowski admits, however, that his explanation is no more than a guess that is not grounded in the facts or evidence presented in this case. (See Tr. 213:20-21 ("How the hotel is assigning [its] IP addresses and their uses that they use them for, I do not know.").) When asked whether there was "any evidence from Mark Hopkins that indicates that traffic in this particular situation was routed outward using a different IP address than .2, or .12," Obuchowski acknowledged that "Mark Hopkins did not supply [this] information in the records" and that he is "not sure

exactly how Mark Hopkins is routing traffic other than that they are using the .12 for web-based traffic." (Tr. 618:1-11.) While Obuchowski's theory is grounded in his "experience in conducting hundreds of investigations, including several hotels," none of those hotels includes the Mark Hopkins. (Tr. 618:6-7.) 2FA also challenges Obuchowski's "re-routing" theory by pointing to several e-mails from Salyards to Cuttill between April 20 and April 22, 2009, all originating from Salyards' Mark Hopkins Hotel IP address ending in .12, not .2. (DX 7 at 11015-20; Tr. 598:21-600:17.)

Fifth, 2FA refutes Passlogix's contention that Collier was engaged in activities that would have prevented him from sending the April 13 e-mail. With respect to evidence of Collier installing a printer on his Passlogix laptop while he claims to have been at 2FA, Collier made clear that he sent the April 13 e-mail from his personal, not Passlogix, laptop. (Collier Dep. 62:6-8; Opp'n Mem 21.) The fact that a printer was being installed and websites were visited on Collier's work computer at the time Collier claims to have been at 2FA does not mean that Collier could not have sent the April 13 e-mail from 2FA's office using his personal computer. While Passlogix contends that Collier was e-mailing Jennifer Kilmer from Collier's Passlogix e-mail account at the time he claims to have been at 2FA's office writing and transmitting the April 13 e-mail,

Cuttill clarified—and the Court agrees—that Collier's e-mail correspondence with Kilmer occurred between 1:23 p.m. CDT and 2:27 CDT, which was before Collier's stated arrival at 2FA's offices around 3 p.m. (Tr. 49:16-51:11, 529:23-531:11; PX 56.) With respect to Collier's thirteen-minute phone call with Salyards from 3:02 to 3:15 p.m. CDT, Cuttill's testimony that Collier arrived at 2FA's office around 3:00 p.m. CDT, "give or take maybe 15 minutes," leaves open the possibility that Collier arrived around 2:45 p.m. and finished his ten-minute (or so) conversation with Cuttill before beginning the call with Salyards. (Tr. 594:10-25; PX 45 at CC10, Item 212.) With respect to evidence that Collier was on the phone with Wardell during the time he claims to have been at 2FA, besides the prospect of multi-tasking, there is a seven-minute gap between when the Hush account was set up at 3:32 p.m. CDT and the start of Collier's call with Wardell at 3:39 p.m. CDT, leaving sufficient time to draft a two-paragraph e-mail. (PX 45 at CC10, Item 213; Tr. 221:11-24.) Moreover, the call ended at 3:55 p.m. CDT, leaving four more minutes before the e-mail was transmitted. (PX 45 at CC10, Item 213; Tr. 222:6-12.)

iii. Passlogix Fails to Present Clear and Convincing Evidence that Salyards Authored the April 13 E-mail

After reviewing all of the evidence in this case, including Collier's three-hour videotaped deposition, the Court holds that

Passlogix has not presented clear and convincing evidence that Salyards authored the April 13 e-mail. Virtually every piece of evidence Passlogix presents is rebutted by 2FA. Importantly, the Court finds Collier's admission to authoring the April 13 e-mail credible.[6] Collier's motive for sending the April 13 e-mail is logical, he matches the profile of the author,[7] and his testimony regarding his subsequent log-ins is corroborated by the Hush logs.[8] Although some inconsistencies remain with respect to Collier's confession, they do not amount to clear and convincing evidence that Salyards authored the e-mail. For instance, Collier stated that he set up the Hush account "a few days before the [April 13] e-mail was sent," yet the Hush logs indicate that the account was set up just twenty-seven minutes before the e-mail was sent. (Collier Dep. 84:10-12, 85:20-86:1;

[6] Passlogix claims that Collier's confession is not credible because Collier previously "disavow[ed] any knowledge of the emails to Passlogix and its lawyers." (Mem. 20.) However, prior to his December 2, 2009 deposition, Passlogix never asked Collier directly whether he sent the April 13 e-mail. (Collier Dep. 80:8-82:5.)

[7] The April 13 e-mail, which was sent on a Monday, refers to the author being on a "call this morning." (PX 2.) Boroditsky testified that Passlogix has a weekly sales call on Mondays. (Tr. 72:13.) While Boroditsky did not know whether Collier was on the call that Monday, April 13, he acknowledged that Collier "has been on those calls." (Tr. 72:17-22.) Salyards, on the other hand, was not supposed to be on those calls. (Tr. 72:15-16.) Boroditsky also stated that the topic of Oracle being brought into the Wal-Mart account "could have been raised" during those Monday sales calls, further linking Collier to the April 13 e-mail. (Tr. 72:23-25.)

[8] Collier testified that after sending the April 13 e-mail, he logged into Hush "[s]ix, maybe seven times" and that the last time he accessed the Hush account "may have been two weeks after [the April 13 e-mail] was sent." (Collier Dep. 86:2-4, 89:2-6.) This testimony largely is consistent with the Hush logs, which indicate nine log-ins to Hush after the April 13 e-mail was sent and show a final log-in on April 27, 2009, fourteen days after the April 13 e-mail was sent. (PX 49.)

see also PX 44 ¶ 6; PX 49.) Also, the password that Collier provided did not match the password used to access Hush. (See Collier Dep. 84:17-85:19; PX 41 & 44 ¶ 5.) However, Collier admitted that he was not sure whether the password he provided was correct and, because there are no records from Hush indicating what the actual password was, the Court does not know whether the password Collier offered was close to the actual password used. (Collier Dep. 85:17-19; PX 41.) In any event, Collier's inaccuracies about the date the Hush account was created and the password he used to create the account do not convince the Court that Collier is lying. For example, Passlogix's own expert admitted that he too could not recall when he set up his more recent Hush test account and what password he assigned to it. (Tr. 235:24-236:5.)

As discussed earlier, the Court does not credit Obuchowski's conclusion that the kind of IP spoofing at issue here is technologically impossible. See supra. Therefore, given Collier's equivocation about the program that he used to spoof Salyards' IP address, Obuchowski's testimony regarding the MAC IP Change program's inability to spoof IP addresses to the degree done here—which the Court credits—is not dispositive of the fact that IP spoofing could not, and did not, happen. (Collier Dep. 86:23-25; Tr. 242:5-11; PX 44 ¶¶ 3-4.)

With respect to how Collier spoofed an IP address similar to the one that the Mark Hopkins Hotel assigned to Salyards, Collier states that the only way he could have used an IP address similar to that of the Mark Hopkins Hotel is if he copied it from an e-mail header that Salyards sent to Collier from the Hotel. (Collier Dep. 93:24-94:1.) In an affidavit submitted to the Court, Salyards states that on April 19, 2009, he sent an e-mail to Collier "from the Mark Hopkins hotel upon [his] arrival in San Francisco via Outlook." (PX 43 ¶ 5(e).) If true, Salyards would have sent this e-mail using a lower level of internet service, which is the only type of internet service purchased by Salyards on April 19. (PX 38 at IHG7-8.) However, this level of internet service was linked to a computer with a MAC address different than Salyards' computer. (Id.) Thus, there is a gap in the record concerning how Collier was able to spoof Salyards' IP address from the Mark Hopkins Hotel using the April 19 e-mail that Salyards allegedly sent. The record also is bare with respect to whether Salyards and Collier may have communicated through remote means, such as a blackberry device, and, if so, what IP address would appear in the e-mail headers of those e-mails. These remaining questions, however, do not amount to the clear and convincing evidence that Passlogix needs to present to prove that Salyards wrote the

April 13 e-mail and used it in an attempt to commit a fraud on the Court.

c. September 3 E-mail

The September 3 e-mail, which was sent the day after Passlogix submitted its opposition to 2FA's motion for a preliminary injunction, accuses Passlogix of using 2FA's and Imprivata's intellectual property in violation of "contractual and ethical obligations." (PX 1.) The anonymous author claims to have transitioned to Passlogix "earlier this year" and to have over fifteen years of development experience. (Id.) The e-mail contains two attachments consisting of Passlogix's confidential technical specifications for a project under development—the dissemination of which "created a serious risk of competitive harm and lost investment for Passlogix." (Mem. 6.) Passlogix seeks sanctions for 2FA's affirmative use of the September 3 e-mail "as negotiating leverage before the settlement conferences on September 16 and October 1, 2009" and for 2FA's "interject[ing] the email into the case as pretext for demanding broad document and deposition discovery into Passlogix's operations." (Id.)

i. Evidence Presented by Passlogix

Like the April 13 e-mail, Passlogix's strongest evidence that Salyards authored the September 3 e-mail are the Hush logs, which indicate that the September 3 e-mail was sent from 2FA's office IP address (70.114.246.62). (See PX 48.) Passlogix also points to Obuchowski's conclusion that there is no software on the market that can be used to spoof a public IP address, including 2FA's office IP address, and that the e-mail headers from the September 3 e-mail show no indicia of spoofing. (Mem. 10; Reply 4-5; Tr. 164:6-19, 168:21-169:16, 242:12-16, 616:20-617:4, 623:17-624:2; PX 36 ¶¶ 14-15.) Passlogix states that given the timing and subject matter of the September 3 e-mail, as well as the Hush logs, it is clear that Salyards sent the e-mail to garner a favorable settlement and to expand discovery. (Mem. 6.) Moreover, because the September 3 e-mail alleges that Passlogix misappropriates the intellectual property of third parties, attaches two proprietary Passlogix documents, and was sent to a third-party business entity that Passlogix has a commercial relationship with, Salyards clearly sought to harm Passlogix's business relations in sending the e-mail. (Id.) Passlogix asserts that Salyards obtained the proprietary attachments either from an anonymous e-mail that Salyards claims to have received in June or July 2009, which purportedly contained one of the attachments, or through his secretive

relationship with Collier. (Tr. 137:17-22, 139:15-21, 436:14-437:2.)

Passlogix insists that 2FA's suggestion that a former Passlogix employee, Joseph Robinson, authored the September 3 e-mail is speculative and inadmissible and that the factual contentions in the September 3 e-mail belie any suggestion that Robinson was the author. (Mem. 11.) First, Passlogix states that its internal investigation concluded that that the claims in the September 3 e-mail were false and that no individual at Passlogix, including Robinson, identified any inappropriate request to utilize intellectual property from third parties. (Tr. 35:10-21, 36:17-22; PX 34 & 35.) Second, the author of the September 3 e-mail refers to receiving a "monthly paycheck" from Passlogix, but Robinson was paid semi-weekly. (Tr. 47:24-48:6, 140:12-13; PX 1.) Third, the September 3 e-mail's author refers to having fifteen years of development experience, but Boroditsky maintains that Robinson had ten years of development experience because Robinson's first five years in the computer technology field consisted of "lesser roles that would not be claimed as software developer roles." (Tr. 48:7-11, 93:10-94:5, 101:16-102:12; PX 1.) Fourth, while the author states that he intends to stop assisting on the SAW project, Robinson continued to work on this project diligently and never raised an issue about the misuse of intellectual property. (Tr. 48:12-15,

139:5-8.) Finally, Robinson and Salyards had no communication with one another, including via e-mail, such that Robinson would have known Salyards' IP address. (Tr. 449:10-18 (Salyards testifying that he never communicated with Robinson in any way).)

Passlogix also contends that Salyards' September 3 alibi does not hold up to scrutiny. Salyards testified that he was at a restaurant with his family and friends when the September 3 e-mail was sent, thereby refuting any claim that he authored the e-mail. (Tr. 433:8-435:19.) Three of Salyards' restaurant companions, as well as Salyards' wife, submitted affidavits and sat for depositions to confirm Salyards' whereabouts on the afternoon of September 3. (DX 1 (2FA Ltr. 10/29/09 at 4 & Ex. 2).) Passlogix, however, contends that the "recollections from these friendly witnesses . . . each of whom arrived and left at different times . . . are inconsistent and contradictory." (Mem. 13.) While Salyards claims that he left his office for the restaurant "at like 3:30 or so" (Tr. 434:2-9), one friend recalled Salyards arriving at "approximately 3:15" (Posey Dep. 16:15-17), another friend recalled Salyards arriving at "3:15, 3:30ish" (Dunson Dep. 14:10-12), the third friend did not "remember what time [Salyards] and his family got there" (Dismore Dep. 9:7-8), and all Salyards' wife could recall was

that she arrived sometime that afternoon and believes Salyards was there already (A. Salyards Dep. 6:9-21).

ii. Evidence Rebutted by 2FA

2FA insists that Salyards could not have sent the September 3 e-mail because he did not have access to the proprietary Passlogix documents that were attached to it. (Opp'n Mem. 5-7.) 2FA also contends that the content of the e-mail and other corroborating evidence point to Robinson as the author. First, 2FA refers to Collier's testimony that, in June 2009, Robinson expressed concerns to him that reflect the concerns in the September 3 e-mail. (Collier Dep. 66:3-67:4, 77:17-78:24.) Specifically, Collier e-mailed Robinson on June 17, 2009, asking him to "take a quick look at the code samples that [Robinson] worked on late last year" at IdentiPHI. (DX 16 at PL96158; see also Collier Dep. 98:21-22.) Robinson was concerned about working on code that he did not write while at Passlogix, and raised the issue with his boss, Cory Womacks, who also hesitated about working on the code. (DX 16 at PL96148 & PL96157-58.) Collier spoke with Robinson over the phone to explain that he was asking for "development assistance for a customer that . . . we were attempting to transition . . . legally and ethically, from IndentiPHI to Passlogix, and [he] needed support that only the developer [Robinson] could provide." (Collier Dep. 77:21-

25.) Collier says that he told Robinson to take up his issues with Boroditsky and, otherwise, abandoned his request and "never spoke to [Robinson] again." (Id. 98:19-99:21.) Contrary to Passlogix's assertion that 2FA relies only on Collier's speculation about Robinson being the author of the September 3 e-mail, 2FA points to an e-mail chain between Collier, Robinson, and Womacks, to corroborate Collier's version of events. (See DX 16 at PL96148-49 & PL96157-58.) Also, Passlogix's notes from its internal investigation indicate that both Robinson and Womacks recalled Collier requesting Robinson's help with the aforementioned code, further corroborating Collier's deposition testimony. (PX 35 at PL95991.)

Collier also testified to speaking with Robinson about Hush and about spoofing Salyards' IP address. Collier states that when Robinson expressed concern about working on certain code, Collier suggested that Robinson raise the issue with Boroditsky or, alternatively, send an e-mail through Hush since "[t]hey won't know who you are." (Collier Dep. 68:7-16.) Importantly, Collier revealed to Robinson that he used Salyards' IP address when he sent his own anonymous e-mail, though he did not tell Robinson what that IP address was. (Id. 98:14-18.)

Second, 2FA states that Salyards was not in 2FA's office when the September 3 e-mail was sent and several witnesses have corroborated that he was with them at a restaurant. (Tr. 433:8-

435:19; Opp'n Mem. 12.) The fact that the witnesses' testimony regarding the timeline was not identical only indicates "that nothing was rehearsed, and three of the witnesses placed Mr. Salyards at the restaurant at the crucial time, recalling what time he arrived and where they sat." (Opp'n Mem. 12.)

Third, 2FA contends that the spelling of certain words in the September 3 e-mail indicates that the author may have had a British or Canadian background, as Robinson does.[9] (Opp'n Mem. 15.) However, 2FA submitted dozens of Robinson's work e-mails, none of which uses the "s" spelling. (Compare PX 1 (anonymous author spelling "organisation" and "utilise" with an "s"), with DX 16 at PL96120 (Robinson spelling "organization" and "serialization" with a "z").) In any event, spelling is not dispositive of identity in this case, since one can impersonate British or Canadian spelling easily by substituting an "s" for a "z" in many common words.

Fourth, 2FA maintains that additional details in the September 3 e-mail refute any claim that Salyards was the author. The author of the September 3 e-mail misspells the e-mail address of Shaun Cuttill—Salyards' long-time business

[9] At the evidentiary hearing, 2FA called Dr. Alan Perlman, a purported expert in linguistics, to testify that Salyards did not author the September 3 e-mail because the language used in the e-mail is inconsistent with his writings. Pursuant to its gatekeeping function under Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993), the Court declined to qualify Dr. Perlman as an expert and, therefore, gives no weight to his testimony in this decision. (See Tr. 259:14-260:5, 261:1-4.)

partner—by using only one "t" instead of two. (Opp'n Mem. 12; Tr. 436:2-10; PX 1.) Additionally, 2FA insists that if Robinson's early technical experience is counted, he has exactly fifteen years of development experience, as stated in the September 3 e-mail. (Opp'n Mem. 13; PX 1 & 21 at PL96028-30; Tr. 80:7-81:5.) Also, as the author of the September 3 e-mail represents, Robinson transitioned to Passlogix earlier in 2009 from another company. (Opp'n Mem. 13; PX 1.) There is no dispute that Robinson had access to the attachments to the September 3 e-mail, since Boroditsky confirmed that Robinson was one of four Canadian developers that Passlogix hired from IndentiPHI to work on the v-GO SAW program. (Tr. 79:1-5, 510:23-511:1; Opp'n Mem. 13; PX 1.) 2FA also contends that the anonymous author's forward-looking statement expressing an intention to leave Passlogix after securing alternative employment is consistent with Robinson's intentions. (Opp'n Mem. 14; PX 1.) 2FA states that Robinson intended to stay at Passlogix until October 1, 2009, so that he could receive his $10,000 retention bonus. (PX 21 at PL96025; Tr. 511:8-512:6; Opp'n Mem. 14.) The retention bonus benchmark and forward-looking statement also correspond with Robinson's subsequent termination on October 15, 2009, for abandoning his position due to unexcused absences. (DX 25; Tr. 515:25-516:2.) Passlogix counters that Robinson continued to assist on the SAW project

until his unexcused absences in late September and that, as far as anyone knows, Robinson has not secured alternative employment. (Tr. 48:12-15.)

iii. Passlogix Fails to Present Clear and Convincing Evidence that Salyards Authored the September 3 E-mail

After reviewing all of the evidence related to the September 3 e-mail, the Court holds that Passlogix has not presented clear and convincing evidence that Salyards authored the September 3 e-mail. 2FA rebuts nearly all of Passlogix's evidence and presents a colorable counter-narrative that Robinson may have authored the September 3 e-mail. This counter-narrative is not limited to Collier's speculation, as Passlogix suggests, but rather is corroborated in part by e-mail correspondence and Passlogix's internal investigation. (See DX 16 at PL96148-49 & PL96157-58; PX 35 at PL95991.) While gaps undoubtedly remain regarding the identity of the author of the September 3 e-mail, 2FA does not bear the burden to prove that someone other that Salyards authored the September 3 e-mail; rather, Passlogix bears the burden to prove that Salyards was the author. Because Passlogix fails to present clear and convincing evidence that Salyards authored the September 3 e-mail, the Court holds that Salyards did not commit a fraud on the Court.

3. 2FA Has Failed to Establish that Passlogix Committed a Fraud on the Court

2FA asserts that by alleging that Salyards committed a fraud on the court when faced with evidence to the contrary, Passlogix "fabricated accusations to interfere with the Court's ability impartially to adjudicate 2FA's counterclaims and it[s] claim of misappropriation," thereby engaging in its own fraud on the court. (Opp'n Mem. 33.) To establish its fraud on the court claim, 2FA must present clear and convincing evidence that Passlogix brought its allegation against Salyards in bad faith—that is, knowing that it was false. See McMunn, 191 F. Supp. 2d at 445 (stating that a fraud on the court "occurs where a party has acted knowingly in an attempt to hinder . . . his adversary's defense of the action") (citation and internal quotation marks omitted); Skywark, 1999 WL 1489038, at *14 (same); see also Schlaifer Nance & Co., Inc. v. Estate of Warhol, 194 F.3d 323, 338 (2d Cir. 1999) ("Bad faith can be inferred when the actions taken are so completely without merit as to require the conclusion that they must have been undertaken for some improper purpose.") (citation and internal quotation marks omitted). Fraud on the court will not lie where the alleged misconduct merely consists of "an advocate's view of the evidence, drawing all inferences favorable to the [client] and

against the [adversary]." Intelli-Check, 2005 WL 3533153, at *12.

2FA has not shown that Passlogix's allegation of fraud on the Court was brought for an improper purpose. Contrary to 2FA's allegations, there is no clear and convincing evidence of an "unconscionable scheme" by Passlogix to delay the litigation; rather, Passlogix's allegations were based upon "an advocate's view of the evidence, drawing all inferences favorable to the [Passlogix] and against [Salyards]." Id.; see also TVT Records v. Island Def Jam Music Group, 447 F. Supp. 2d 311, 315 (S.D.N.Y. 2006) (holding that "even if [plaintiff] pressed this motion [for sanctions] with utmost zeal and certain aspects of it rest on grounds that are somewhat tenuous, . . . the Court is not persuaded that [plaintiff's] application was frivolous, objectively unreasonable or pursued in bad faith"). Passlogix brought its fraud on the court allegation only after conducting an internal investigation and obtaining subpoenaed records from Hush, which appeared to provide objective evidence linking Salyards to both anonymous e-mails. It was not until after the Court granted the parties further discovery at the November 9 preliminary hearing that additional evidence arose challenging the conclusions drawn from the Hush logs and supporting 2FA's defense of IP spoofing. Nonetheless, even in the face of this subsequent discovery, Passlogix's continued presentation of its

claim against Salyards was not "frivolous, objectively unreasonable or pursued in bad faith" because, as already discussed, the competing evidence does not conclusively support that Salyards was not the author of the e-mails; rather, it hinders Passlogix's ability to show, by clear and convincing evidence, that Salyards was the author. TVT Records, 447 F. Supp. 2d at 314, 315 (holding that "the record lacks clear and convincing evidence to support a finding that [defendant] acted in actual bad faith at the time his . . . submission was made"). The Court holds, therefore, that 2FA has failed to establish that Passlogix committed a fraud on the Court by pursuing its claims against Salyards.

4. 2FA's Request to Amend Its Complaint to Assert a Claim for Malicious Institution of Civil Proceedings is Denied

2FA requests leave to amend its counterclaims to include a claim against Passlogix for malicious institution of civil proceedings. (Opp'n Mem. 35.) 2FA states that, prior to bringing its fraud on the court allegation against Salyards, Passlogix possessed evidence indicating that Salyards did not send either anonymous e-mail but, nonetheless, continued to pursue its claim even after obtaining further evidence during discovery that Salyards was innocent. (Id. 34.)

Courts are instructed to "freely give leave [to amend] when justice so requires." Fed. R. Civ. P. 15(a)(2); see also Holmes v. Grubman, 568 F.3d 329, 334 (2d Cir. 2009). Leave to amend need not be granted, however, where the proposed amendment would be futile. See Advanced Magnetics, Inc. v. Bayfront Partners, Inc., 106 F.3d 11, 18 (2d Cir. 1997) (Kearse, J.). In addition to futility, "'[a] district court has discretion to deny leave for . . . bad faith, undue delay, or undue prejudice to the opposing party.'" Holmes, 568 F.3d at 334 (quoting McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 200 (2d Cir. 2007)).

To recover on a claim of malicious prosecution under New York law, Salyards must establish that: (1) Passlogix either commenced or continued a criminal or civil proceeding against him; (2) the proceeding terminated in his favor; (3) there was no probable cause for the criminal or civil proceeding; and (4) the criminal or civil proceeding was instituted with actual malice. See von Bulow v. von Bulow, 657 F. Supp. 1134, 1140 (S.D.N.Y. 1987); Rosemont Enters., Inc. v. Random House, Inc., 261 F. Supp. 691, 695 n.11 (S.D.N.Y. 1966); see also Russo v. New York, 672 F.2d 1014, 1018 (2d Cir. 1982), on reh'g, 721 F.2d 410 (2d Cir. 1983); Brady v. Penn Cent. Transp. Co., 406 F. Supp. 1239, 1242 (S.D.N.Y. 1975). A favorable conclusion does not necessarily mean that there was no probable cause for the institution of a claim. See Brady, 406 F. Supp. at 1242

(holding that "[t]he fact that the indictment was discontinued against the plaintiffs does not, in and of itself, constitute a lack of probable cause for the initial arrests"). The New York Court of Appeals has stated clearly that a litigant "may act on evidence which would seem reasonably to justify making a charge, and the prosecution will not be malicious if he was mistaken about the true meaning of the evidence." Munoz v. City of N.Y., 18 N.Y.2d 6, 9, 218 N.E.2d 527 (1966).

2FA's request to amend its complaint to add a malicious prosecution charge is denied as futile. While Salyards can establish the first two elements of a malicious prosecution claim, he cannot establish the latter two elements of lack of probable cause and malice. As already discussed, in bringing the instant allegations, Passlogix reasonably relied on the Hush logs, which showed objective evidence that Salyards was involved in transmitting both the April 13 and September 3 e-mails. While Passlogix pressed forward notwithstanding evidence uncovered in future discovery, it did so in good faith based upon "an advocate's view of the evidence." Intelli-Check, 2005 WL 3533153, at *12; see also Sauer v. Xerox Corp., 5 Fed. Appx. 52, 57 (2d Cir. 2001) (affirming district court's denial of attorneys' fees where, "although ultimately adjudged to be without merit, [plaintiff's] suit cannot be fairly characterized as 'entirely without color and [undertaken] for reasons of

harassment or delay or for other improper purposes'" (citation omitted)); Menashe v. V Secret Catalogue, Inc., 409 F. Supp. 2d 412, 427 (S.D.N.Y. 2006) (rejecting claim for attorneys' fees where there was "nothing in [the] record to suggest that" the unsuccessful claim was brought "in bad faith, vexatiously, wantonly, or for oppressive reasons" (internal quotation marks omitted)). Passlogix, therefore, had probable cause to commence and continue its fraud on the court allegation against Salyards because of the Hush logs, its expert's testimony concluding that no IP spoofing occurred, and remaining gaps concerning the identity of the author(s) of the anonymous e-mails. Passlogix lacked malice in commencing and continuing its claim because it acted on evidence that "seem[ed] reasonably to justify making a charge," even if Passlogix ultimately "was mistaken about the true meaning of the evidence." Munoz, 18 N.Y.2d at 9.

For the foregoing reasons, 2FA's request to amend its counterclaims to assert a cause of action for malicious prosecution against Passlogix is denied on grounds of futility.

II. Spoliation of Evidence

Passlogix alleges that because Salyards and Cuttill admit to failing to implement a litigation hold notice and to deleting certain documents during the pendency of this litigation, they should be sanctioned for spoliation of evidence. (Mem. 31.)

The destroyed documents include: (1) an anonymous e-mail received by Salyards in June or July 2009 containing an attachment of Passlogix functional specifications; (2) at least 143 written communications between Salyards and Collier; and (3) 2FA network and computer logs from Cuttill's inspection of 2FA's computers and computer network. (Id. 31-32.) As a result of 2FA's purported spoliation of evidence, Passlogix asks for three forms of relief. First, Passlogix requests that an adverse inference be drawn that the deleted documents would have been harmful to 2FA and beneficial to Passlogix. (Id. 33.) Second, Passlogix requests that 2FA be precluded from making arguments implicating the discarded documents. (Id.) Third, Passlogix asks that Salyards be responsible for the cost of Passlogix's investigation, which was more costly and protracted as a result of Salyards' destruction of documents. (Id. 34.)

A. Legal Standard

"Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, -- F. Supp. 2d --, 2010 WL 184312, at *4 (S.D.N.Y. Jan. 15, 2010); see also West v. Goodyear Tire & Rubber Co., Inc., 167 F.3d 776, 779 (2d Cir.

1999); Scalera v. Electrograph Sys., 262 F.R.D. 162, 170 (E.D.N.Y. 2009); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 430 (S.D.N.Y. 2004) ("Zubulake V"). "The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct 'which abuses the judicial process.'" Pension, 2010 WL 184312, at *4 (quoting Chambers, 501 U.S. at 45). A party seeking sanctions for spoliation of evidence must establish:

> (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

Zubulake V, 229 F.R.D. at 430; see also Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 107-11 (2d Cir. 2001); Scalera, 262 F.R.D. at 170-71. The Court analyzes each of these three elements below.

1. Duty to Preserve

A litigant has the "duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the

subject of a pending discovery request." Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991) (citation omitted); see also Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998); In re NTL, Inc. Sec. Litig., 244 F.R.D. 179, 193 (S.D.N.Y. 2007). "[N]o duty to preserve arises unless the party possessing the evidence has notice of its relevance." Turner, 142 F.R.D. at 72-73. A party is on notice to preserve relevant documents "when litigation is reasonably anticipated," Pension, 2010 WL 184312, at *1, and "at least by the time the complaint [is] served," Turner, 142 F.R.D. at 73. "This obligation to preserve relevant evidence exists whether or not the evidence has been specifically requested in a demand for discovery." Scalera, 262 F.R.D. at 171; see also Barsoum v. N.Y.C. Hous. Auth., 202 F.R.D. 396, 400 (S.D.N.Y. 2001).

After obtaining notice of the litigation, a party "'must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents.'" Pension, 2010 WL 184312, at *4 (quoting Treppel v. Biovail Corp., 249 F.R.D. 111, 118 (S.D.N.Y. 2008)); see also Toussie v. County of Suffolk, No. 01 Civ. 6716, 2007 WL 4565160, at *7 (E.D.N.Y. Dec. 21, 2007) ("[O]nce the duty to preserve attaches, at a minimum, a litigant is expected to 'suspend its routine document and retention/destruction policy and to put in place a litigation hold.'") (quoting Zubulake v.

UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) ("Zubulake IV")). The requirement to issue a written litigation hold notice has been in place in this District since the Zubulake V decision in July 2004. See Pension, 2010 WL 184312, at *10 (stating that plaintiffs' failure to institute a litigation hold notice by 2005 when the action was transferred to the Southern District of New York was grossly negligent in light of the requirement that "was clearly established in this District by mid[-]2004"). "The preservation obligation runs first to counsel, who has 'a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction.'" Chan v. Triple 8 Palace, Inc., No. 03 Civ. 6048, 2005 WL 1925579, at *6 (S.D.N.Y. Aug. 11, 2005) (quoting Turner, 142 F.R.D. at 73); see also Zubulake V, 229 F.R.D. at 439 ("[C]ounsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. . . . In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored.").

Once on notice of litigation, "the failure to issue a written litigation hold constitutes gross negligence because

that failure is likely to result in the destruction of relevant information." Pension, 2010 WL 184312, at *3 (emphasis in original); see also Crown Castle USA Inc. v. Fred A. Nudd Corp., No. 05 Civ. 6163T, 2010 WL 1286366, at *13 (W.D.N.Y. Mar. 31, 2010) (holding plaintiff grossly negligent for failing to implement a litigation hold, which led to the destruction of documents); Richard Green (Fine Paintings) v. McClendon, 262 F.R.D. 284, 290 (S.D.N.Y. 2009) ("[T]he failure to implement a litigation hold is, by itself, considered grossly negligent behavior."); Toussie, 2007 WL 4565160, at *8; Chan, 2005 WL 1925579, at *7 ("[T]he utter failure to establish any form of litigation hold at the outset of litigation is grossly negligent."). In one case, however, this District has found negligence, rather than gross negligence, when a party failed to institute a litigation hold but then corrected its failure. See Pension, 2010 WL 184312, at *18 n.179 (holding seven plaintiffs negligent, rather than grossly negligent, for failing to issue a litigation hold by 2005 where all plaintiffs issued such a notice by 2007 and where instituting the litigation hold in 2005 may not have made any difference because the electronic records that existed in 2003 very likely would have been lost or destroyed by 2005).

2. Culpable State of Mind

In the spoliation context, a culpable state of mind includes ordinary negligence. See Zubulake V, 229 F.R.D. at 431; see also Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002). "When evidence is destroyed in bad faith (i.e., intentionally or willfully), that fact alone is sufficient to demonstrate relevance." Zubulake V, 229 F.R.D. at 431; see also Residential Funding, 306 F.3d at 108-09. By contrast, when the destruction is negligent, grossly negligent, or reckless, relevance must be proven by the party seeking sanctions. See Zubulake IV, 220 F.R.D. at 221 ("[B]ecause UBS's spoliation was negligent and possibly reckless, but not willful, [plaintiff] must demonstrate that a reasonable trier of fact could find that the missing e-mails would support her claims."); see also Richard Greene, 262 F.R.D. at 291.

"No matter what level of culpability is found, . . . the spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information." Pension, 2010 WL 184312, at *5. To show prejudice, "[t]he moving party usually sets forth some type of extrinsic evidence as to the content of missing materials which demonstrates the extent to which such materials would have been harmful to the spoliator." Skeete v. McKinsey & Co., Inc., No. 91 Civ. 8093, 1993 WL 256659, at *7 (S.D.N.Y. July 7, 1993) (Leisure, J.). "If the spoliating party offers proof that there

has been no prejudice, the innocent party, of course, may offer evidence to counter that proof." Pension, 2010 WL 184312, at *5.

3. Relevance

In the spoliation context, relevance "means something more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence." Chan, 2005 WL 1925579, at *7; see also Residential Funding, 306 F.3d at 108-09. A discarded document is relevant where a reasonable trier of fact could find that the document either would harm the spoliator's case or support the innocent party's case. See Port Auth. Police Asian Jade Soc'y of N.Y. & N.J. Inc. v. Port Auth. of N.Y. & N.J., 601 F. Supp. 2d 566, 570 (S.D.N.Y. 2009) ("'[R]elevant' means that the evidence must be of the sort that a reasonable jury could find harmful to the spoliator's case."); Zubulake V, 229 F.R.D. at 430 (stating that a discarded document is "relevant" to the victimized party's "claim or defense" where "a reasonable trier of fact could find that [the missing document] would support that claim or defense"). "[R]elevance 'may be inferred if the spoliator is shown to have a sufficiently culpable state of mind.'" Scalera, 262 F.R.D. at 178 (quoting Chan, 2005 WL 1925579, at *8). To have a sufficiently culpable state of mind warranting a relevance inference, the spoliator must have acted

in bad faith—that is, intentionally or willfully. See In re Methyl Tertiary Butyl Ether Prods. Liab. Litig., 643 F. Supp. 2d 482, 496 (S.D.N.Y. 2009); Zubulake V, 229 F.R.D. at 431; Zubulake IV, 220 F.R.D. at 221; Turner, 142 F.R.D. at 77. "Although many courts in this district presume relevance where there is a finding of gross negligence, application of the presumption is not required." Pension, 2010 WL 184312, at *5; see also Residential Funding, 306 F.3d at 109 ("[A] showing of gross negligence in the destruction or untimely production of evidence will in some circumstances suffice, standing alone, to support a finding that the evidence was unfavorable to the grossly negligent party."); Treppel, 249 F.R.D. at 121-22 ("While it is true that under certain circumstances 'a showing of gross negligence in the destruction or untimely production of evidence' will support [a relevance] inference, the circumstances here do not warrant such a finding, as the defendants' conduct 'does not rise to the egregious level seen in cases where relevance is determined as a matter of law.'" (quoting Residential Funding, 306 F.3d at 109 and Toussie, 2007 WL 4565160, at *8)).

In the absence of bad faith destruction of evidence, "the moving party may submit extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it." Chan, 2005 WL 1925579, at *8. Moreover, "when the

spoliating party [is] merely negligent, the innocent party must prove both relevance and prejudice in order to justify the imposition of a severe sanction." Pension, 2010 WL 184312, at *5; see also Byrnie, 243 F.3d at 108 ("[T]he burden falls on the 'prejudiced party' to produce 'some evidence suggesting that a document or documents relevant to substantiating [its] claim would have been included among the destroyed files.'" (quoting Kronisch, 150 F.3d at 128)). The innocent party may do so by presenting "'extrinsic evidence tending to show that the destroyed e-mails would have been favorable to [its] case.'" Pension, 2010 WL 184312, at *5 (quoting Toussie, 2007 WL 4565160, at *8).

B. Application

To establish that Salyards engaged in spoliation of evidence by deleting the documents at issue, Passlogix must show by a preponderance of the evidence that, for each category of documents: (a) Salyards had a duty to preserve the documents at the time they were destroyed; (b) Salyards destroyed the documents with a culpable state of mind; and (c) the destroyed documents were relevant to Passlogix's claim or defense. See Pension, 2010 WL 184312, at *5; Zubulake V, 229 F.R.D. at 430; Scalera, 262 F.R.D. at 170-71. For the reasons set forth below, the Court holds that although Passlogix has satisfied the first

two elements—duty and culpable state of mind—with respect to all three categories of deleted documents, it has satisfied the final relevance prong only with respect to the latter two: (2) written communications between Salyards and Collier, and (3) logs from Cuttill's investigation of 2FA's computers and computer network. As a sanction for 2FA's spoliation of documents, the Court orders 2FA to pay a fine of $10,000.

1. June/July Anonymous E-mail

Salyards testified at his deposition and at the evidentiary hearing that he received an anonymous e-mail around late June or early July 2009 that included an attachment containing Passlogix functional specifications (the "June/July e-mail"). (Tr. 356:7-22, 357:11-17.) Salyards could not recall the e-mail address from which the June/July e-mail was sent, except that he believed it came from a "hushmail.com" domain name. (Tr. 357:2-10.) After receiving the June/July e-mail, which was sent only to him, Salyards testified that he spent about forty-five minutes to an hour reading the attachment, then showed it to Cuttill. (Tr. 356:10-11, 358:13-19.) After reading and discussing the document, both Salyards and Cuttill decided it was improper for them to have it, so Salyards deleted it without disclosing it to his attorney or Passlogix. (Tr. 358:18-359:2.)

Salyards notes that this attachment was similar to one of the attachments to the September 3 e-mail. (Tr. 436:14-437:2.)

Passlogix first contends that Salyards is lying about the existence of the June/July e-mail "to cover up his role in the other two emails." (PX 33 at 4 n.1.) Passlogix asserts that Salyards' claim that he deleted the attachment to the June/July e-mail is not credible when juxtaposed with Salyards' push "for expansive discovery based on his review of the computer specifications attached to the September 3 E-mail," which, according to Salyards, contained similar content. (Reply Mem. 13.) The Court, however, finds Salyards' testimony about the existence of the June/July e-mail credible because he first testified about the e-mail at a deposition that took place before Passlogix brought its fraud on the court claim, thereby refuting Passlogix's argument that Salyards had a motive to lie about the June/July e-mail to cover-up his role in the other two e-mails. (PX 33 at 4 n.1.)

Alternatively, Passlogix argues that, assuming that the June/July e-mail existed, Salyards engaged in spoliation of evidence by deleting it. Salyards concedes that he deleted the June/July e-mail. (Tr. 357:18-358:5.) 2FA contends that Salyards' deletion of the June/July e-mail is not spoliation because the e-mail "was not evidence when Mr. Salyards deleted it" and "[t]he attachment was a Passlogix document, which is

still in its possession." (Opp'n Mem. 29.) Moreover, 2FA asserts that even if the June/July e-mail "were evidence, it would only help show the misappropriation of intellectual property and is favorable to 2FA." (Id.) 2FA also contends that Salyards' deletion of the June/July e-mail was no different from Boroditsky's, Passlogix's CEO's, request that the recipients of the September 3 e-mail delete that e-mail and its attachments. (Id. 29-30; Tr. 89:15-21.)

a. Duty

The Court holds that 2FA had a duty to preserve the June/July e-mail at the time that Salyards deleted it. According to Salyards, the June/July e-mail contained Passlogix technical specifications that he and Cuttill recognized they should not possess. (Tr. 358:13-359:2.) 2FA states that Salyards' deletion of the June/July e-mail was not spoliation because "[t]he attachment was a Passlogix document, which is still in [Passlogix's] possession." (Opp'n Mem. 29). The significance of the June/July e-mail, however, is not that Passlogix may have a copy of the proprietary attachment, but that the attachment was sent to Salyards. (Tr. 356:10-11.)

"While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed," the June/July e-mail is particularly germane to the underlying

litigation which involves a claim by 2FA that Passlogix misappropriated its intellectual property. Turner, 142 F.R.D. at 72. Although 2FA argues that the June/July e-mail was not evidence when Salyards deleted it, 2FA's duty to preserve extends not only to evidence, but to what "is reasonably calculated to lead to the discovery of admissible evidence" or is "reasonably likely to be requested during discovery." Id. (citation and internal quotation marks omitted); see also Arista Records LLC v. Usenet.com, Inc., 608 F. Supp. 2d 409, 433 (S.D.N.Y. 2009). An e-mail transmitting Passlogix's own propriety information, even if not evidence itself, may lead to the discovery of admissible evidence regarding Passlogix's intellectual property safeguarding practices. See Arista, 608 F. Supp. 2d at 433; Turner, 142 F.R.D. at 72. Because 2FA's duty to preserve documents related to Passlogix's underlying lawsuit attached, at minimum, on December 18, 2008, when Passlogix filed its original complaint, Salyards was on notice of the June/July e-mail's relevance when he deleted it shortly after receiving it in June or July 2009. See Turner, 142 F.R.D. at 73.

For the foregoing reasons, the Court holds that Salyards violated his duty to preserve documents when he deleted the June/July e-mail.

b. Culpable State of Mind

The Court holds that Salyards was grossly negligent in deleting the June/July e-mail. Notwithstanding his obligation to preserve documents, Salyards testified that 2FA never implemented a litigation hold and continues to delete e-mails routinely. (Tr. 353:9-14, 449:23-450:7, 451:11-14; PX 43 ¶ 2.) Passlogix contends that 2FA's failure to implement a litigation hold/document retention notice, standing alone, warrants sanctions. (Mem. 31; Reply Mem. 12.)

As detailed above, "the failure to implement a litigation hold is, by itself, considered grossly negligent behavior." Richard Greene, 262 F.R.D. at 290. Because Salyards admits that 2FA did not, and does not, have a litigation hold/document preservation policy, Passlogix "has clearly satisfied its burden with respect to the second prong of the spoliation test." Id. at 291. Thus, the Court holds that 2FA acted with gross negligence by deleting the June/July e-mail in the absence of a litigation hold during the pendency of this litigation.

c. Relevance

Because there is insufficient evidence indicating that Salyards deleted the June/July e-mail in bad faith, the Court does not infer relevance. Likewise, the Court declines to infer relevance based on 2FA's grossly negligent failure to institute

a litigation hold because 2FA's conduct, in the context of its overall document production in this case, "does not rise to [an] egregious level." Toussie, 2007 WL 4565160, at *8. Therefore, to satisfy the relevance requirement, Passlogix must submit extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it. See Chan, 2005 WL 1925579, at *8.

Although "the burden placed on the moving party to show that the lost evidence would have been favorable to it ought not be too onerous," id. at *7, Passlogix submits no extrinsic evidence tending to show that the June/July e-mail would have been favorable to it. Passlogix states that had the June/July e-mail been preserved, the parties may have been able to track down the IP address and other information identifying the sender and, thereby, test the bonafides of Salyards' IP address spoofing defense. (Mem. 34.) However, the only way the June/July e-mail could be relevant to Passlogix, i.e., support its theory that Salyards is the author of the anonymous Hush e-mails, is if—implausibly—Salyards sent the June/July e-mail to himself. If, on the other hand, the June/July e-mail indicated that someone other than Salyards was the author, then the e-mail would harm, rather than support, Passlogix's theory that Salyards is the author of these anonymous Hush e-mails. Since Passlogix cannot point to extrinsic evidence tending to show

that Salyards authored the June/July e-mail, the Court is "not persuaded on this record that a reasonable [trier of fact] could find that the [June/July e-mail] was harmful" to 2FA or helpful to Passlogix. Adorno v. Port Auth. of N.Y. & N.J., 258 F.R.D. 217, 229 (S.D.N.Y. 2009) (Chin, J.); see also Port Auth. Police Asian Jade Soc'y, 601 F. Supp. 2d at 570 (denying motion for sanctions for spoliation where moving party could not demonstrate that evidence would have been unfavorable to the spoliator); Hamre v. Mizra, No. 02 Civ. 9088, 2005 WL 1083978, at *3 (S.D.N.Y. May 9, 2005) (Leisure, J.) (denying plaintiffs' request for adverse inference where they "did not put forth any evidence" indicating that destroyed documents would corroborate their theory of the case (emphasis in original)). To the extent that Passlogix's investigation into Hush-related e-mail activity was more burdensome and expensive as a result of Salyards' deletion of the June/July e-mail, (Mem. 34), the court discerns no prejudice to Passlogix going to the merits of the case, and Passlogix points to none. See Pension, 2010 WL 184312, at *5.

For the foregoing reasons, the Court holds that although 2FA had a duty to preserve the June/July e-mail and was grossly negligent in deleting it, it did not engage in spoliation of evidence because Passlogix has failed to establish that the e-mail would have been helpful to its claims or defenses or harmful to 2FA's claims or defenses.

2. Written Communications between Collier and Salyards

Passlogix contends that Salyards engaged in the spoliation of evidence by deleting at least 143 written communications with Collier during the pendency of this litigation. (Mem. 31-32.) These destroyed documents consist of at least twelve e-mails, ninety-one text messages, and forty Skype messages.[10] (Id. 31.) Passlogix states that because Collier used his personal, rather than his work, computer to engage in most of these communications, there was no way for Passlogix to obtain a copy of most of these records. (Reply Mem. 13 n.13.) 2FA acknowledges that it did not preserve these written communications, but states that Collier's involvement in this litigation "was only known to 2FA in late November 2009" and that "neither Mr. Salyards nor 2FA had any knowledge, or reason to know, that any documents related to Chris Collier might be relevant in this case, which anyway they are not." (Opp'n Mem. 30.) 2FA also points out that Passlogix has obtained some of the e-mails, phone records, and Skype messages, resulting in no prejudice to Passlogix. (Id.)

To address the discarded the written communications between himself and Collier during the pendency of this litigation,

[10] Skype is an internet software application that, among other features, allows users to engage in instant messaging.

Salyards submits an affidavit outlining their correspondence based on a review of his phone records, travel calendar, and discussions with Cuttill. (PX 43 ¶ 5.) Salyards recalls corresponding with Collier via e-mail "approximately 12 times in 2009" and that "eight of the exchanges were during [Collier's] tenure at Passlogix," which was from April 1, 2009 to November 16, 2009. (Id.) Salyards states that these e-mails generally concern possible business opportunities and consist of statements such as, "let's talk about something. Phone call, let's talk about a lot." (Id. ¶ 3; see also Tr. 440:10-13.) With respect to the content of the unsaved text messages, Salyards states that "they were routinely confirming the ability or inability to answer a call, the arrival at a restaurant at a specific time or our respective locations on the lake," and consisted of phrases such as "I'm leaving, lunch, I'm here, be five minutes." (PX 43 ¶ 13; see also Tr. 440:4-9.)

The Skype records that Passlogix obtained from Collier's work computer indicate that the Skype messages between Salyards and Collier mainly concern lunch plans or social activities. (See PX 50; Tr. 46:1-7, 124:20-127:5.) These Skype records corroborate Salyards' description of the typical Skype exchanges between him and Collier. (See Tr. 442:25-443:10 (Salyards testifying that the typical Skype messages between him and Collier consisted of statements like "you busy," "on the phone,"

"cool," and "where").) Passlogix, however, claims that some of the Skype communications concern topics at issue in the underlying litigation and, therefore, should have been preserved. (Reply Mem. 13.)

Passlogix also points to Collier's secret visits with Salyards at 2FA's office as circumstantial proof that their interactions related to the underlying litigation. Salyards acknowledges that from April 2009 through November 16, 2009, Collier came to 2FA's office at least seven times, but that Salyards "was always under the impression that [Collier] had full endorsement from Passlogix and was acting as a go between" for Passlogix's interest in a software product that 2FA had licensed to HID Global, 2FA's largest customer who also maintains a business relationship with Passlogix. (PX 43 ¶¶ 6 & 5(f)(a).)

a. Duty

Salyards admits that he did not preserve the 143 written communications he had with Collier. (Tr. 354:21-355:25.) Salyards testified that 2FA does not have a document retention policy, that he routinely deletes e-mails and text messages, and that his Skype logs are retained for about two weeks and then are purged automatically. (Tr. 449:23-451:4; PX 43 ¶ 2.)

As already discussed, by December 18, 2008, Salyards had a duty to preserve documents related to the underlying litigation. That duty extends to documents concerning, but not limited to, the misappropriation of intellectual property and the parties' obligations and performance under their licensing agreement. (See generally Compl.; Am. Compl.; Answer & Countercl.) The issue is whether Salyards was on notice that some of his written communications with Collier were probative of the underlying litigation when the communications were deleted. The Court holds that he was.

Salyards' affidavit accounts for at least one e-mail from mid-August 2009, in which Collier asks for Salyards' "help coordinating the development effort with HID" to "get naviGO into [Passlogix's] authenticator program." (PX 43 ¶ 5(g).) NaviGo is a 2FA software product that 2FA licensed to HID Global, 2FA's largest customer, who also maintains a business relationship with Passlogix. (Id. ¶ 5(f)(a).) Salyards states that he referred Collier to two other 2FA employees for assistance, and that he and Collier "had several follow-up conversations on this topic." (Id. ¶ 5(g).) Such an e-mail, which discusses a potential business opportunity between Passlogix and 2FA, is probative of the parties' underlying dispute, which arises from Passlogix's prior licensing of 2FA's software. Passlogix also contends that a Skype message from

April 30, 2009, in which Salyards asks Collier, "do you have access to PLX Adminitrack?" (PX 50 at PL961801), implicates "the very subject of discovery disputes before the Magistrate Judge" and constitutes communication "about product bugs and maintenance matters at issue in the case." (Reply Mem. 13.) Salyards acknowledges that he "talk[ed] to [Collier] about PLX AdminiTrack," which is a "detrack or bug defect tracking system," around the same timeframe that 2FA sent Passlogix a discovery request for "all historical and present AdminiTrack items ever entered." (Tr. 460:17-462:17; PX 63 ¶ 27.) This Skype message relates to a discovery request regarding software maintenance matters at issue in the underlying litigation and, therefore, should have been preserved.

For the reasons above, Salyards had a duty to preserve written communications with Collier pertaining to, at a minimum, 2FA's software and business opportunities with Passlogix as well as maintenance matters related to software at issue in the parties' underlying lawsuit. By failing to preserve such documents, including the aforementioned e-mail and Skype message, Salyards breached his duty to preserve documents.

b. Culpable State of Mind

2FA argues that neither Salyards nor 2FA acted willfully or negligently in deleting the communications with Collier, who was

not involved in this case until late November 2009. (Opp'n Mem. 32.) As already discussed, even if Collier was not involved actively in the instant fraud on the court dispute until late November 2009, at least two of Salyards' written communications with Collier relate to issues involved in the underlying litigation. Salyards' failure to preserve these written communications, in addition to 2FA's overall failure to issue a litigation hold notice, constitutes gross negligence.

c. Relevance

Passlogix provides extrinsic evidence that the written communications that Salyards discarded would support Passlogix's position in the underlying litigation. The April 30, 2009 Skype message, in which Salyards suggests that Collier report a software problem on Passlogix's AdminiTrack system, directly relates to a discovery request in the underlying litigation. However, because Passlogix obtained a copy of these Skype communications from Collier's work computer, it is not prejudiced by their deletion. See Pension, 2010 WL 184312, at *5 ("[T]he spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information."); Ispat Inland, Inc. v. Kemper Envtl., Ltd., No. 05 Civ. 5401, 2006 WL 3478339, at *3 (S.D.N.Y. Nov. 30, 2006) (denying defendant's motion for

sanctions for alleged perjury and spoliation of evidence where, although deponent, in-house counsel at plaintiff corporation, admitted to discarding documents used to refresh his recollection prior to his deposition, defendant's counsel had duplicates in his actual possession at the deposition).

The record provides additional extrinsic evidence that the deleted communications between Salyards and Collier were relevant. The e-mail that Salyards deleted in mid-August 2009, in which Salyards sought to help Collier "get naviGO into [Passlogix's] authenticator program," (PX 43 ¶ 5(g)), provides extrinsic proof that this communication, if preserved, could support Passlogix's defense to 2FA's misappropriation of intellectual property claim. This communication could lead a reasonable factfinder to cast doubt on 2FA's misappropriation claim where 2FA, a purported victim of Passlogix's misappropriation of its intellectual property, pursues a business opportunity with Passlogix involving 2FA's intellectual property in the midst of a lawsuit relating to the fall-out of a prior such relationship. Because Passlogix does not have a copy of this e-mail and because Salyards' description of the e-mail in his affidavit does not supplant the missing document, Passlogix is prejudiced by its deletion.

For the reasons stated above, the Court holds that, in failing to preserve written communications between Salyards and

Collier concerning software maintenance matters and potential business opportunities between 2FA and Passlogix, 2FA engaged in the spoliation of evidence.

3. 2FA's Computer and Network Logs from Cuttill's Investigation

Passlogix alleges that 2FA failed to preserve evidence from Cuttill's personal inspection of 2FA's computers and computer network. (Mem. 32.) 2FA responds that Passlogix was aware of Cuttill's inspection since December 1, 2009, when Cuttill testified about it during his deposition, "but never requested anything from 2FA in this regard, and never made any requests in the several appearances before Judge Dolinger." (Opp'n 32.) Passlogix responds that, during Cuttill's deposition, 2FA's counsel blocked questioning pertaining to Cuttill's investigation, citing attorney client and work product privileges, yet later admitted that counsel was not involved in the investigation. (Mem. 32; Tr. 571:11-20; 12/22/09 J. Dolinger Hr'g Tr. 24:24-28:4.)

At the evidentiary hearing, Cuttill testified that in late October or early November 2009, he interviewed people who had access to 2FA's network on September 3 and checked all of 2FA's computers for evidence of the attachments to the September 3 e-mail and found no evidence that anyone at 2FA sent that e-mail.

(Tr. 572:25-575:5.) He also testified that he interviewed people that he thought had access to 2FA's network in April but did not interview Collier since the interviews were conducted before Collier's confession. (Tr. 573:6-14.) Cuttill did not take notes during his interviews and investigation. (Tr. 573:15-16.) Cuttill also said that he reviewed 2FA's computer logs but did not produce those logs because they were "indiscernible" and "inconclusive." (Tr. 575:6-578:21.) Cuttill explains that the September logs "were tainted" because, by the time he conducted his investigation, "the most recent cookies were all from . . . the second or third week of September" and "[t]here was nothing from September 3rd." (Tr. 577:1-7.) Cuttill testified that during the second or third week of September, he and Salyards had visited Hush "to find out what Hushmail was all about." (Tr. 577:3-16.) Therefore, had these logs been produced, Passlogix "would have come back and said, 'But if he accessed it [in mid-September], what if he accessed it before?' And that wouldn't have been proof of anything." (Tr. 577:11-16.) Then Cuttill said that "[t]here were some security logs that show that Greg Salyards' computer was locked" on September 3, but 2FA did not produce those logs either—even though they appear helpful to 2FA's position—because "[t]hey weren't asked for, and to be honest, we were moving so quickly in this that I - I don't know." (Tr. 578:10-18.)

Cuttill offered to produce these logs with 2FA's post-hearing brief, though the Court has no record of any logs from Cuttill's investigation ever being produced. (Tr. 578:15-19.)

a. Duty

Cuttill admits that his investigation took place after Passlogix sent its letter to the Court accusing Salyards of authoring the anonymous e-mails and, therefore, after 2FA's duty to preserve documents related to the authorship of the April 13 and September 3 e-mails attached. (Tr. 573:10-13.) Even if Passlogix had not requested the logs, as 2FA contends, the duty to preserve documents is not limited solely to documents that are "the subject of a pending discovery request"; rather, the duty extends to documents "reasonably likely to be requested during discovery." Turner, 142 F.R.D. at 72. Since Cuttill affirmatively undertook his investigation, he had a duty to preserve the fruits of that investigation, whether ripe or rotten. Because 2FA requested information from Passlogix's internal investigation, it was reasonable for 2FA to expect that Passlogix, likewise, would request documents related to any investigation 2FA conducted. Even if 2FA no longer had its April 2009 and September 3 computer logs by the time Cuttill conducted his investigation, Cuttill had a duty to preserve the logs that were available—that is, the mid-September logs, which

Cuttill admits were accessible. See Treppel, 249 F.R.D. at 119 ("[I]t is . . . clear that [defendant] should have retained the monthly backup tapes of the relevant servers from the previous year, since these were quite likely to contain files that were later deleted"); Zubulake IV, 220 F.R.D. at 218 ("If a company can identify where particular employee documents are stored on backup tapes, then the tapes . . . should be preserved if the information contained on those tapes is not otherwise available."). 2FA, therefore, breached its duty to preserve documents when it did not retain the computer logs that Cuttill reviewed.

b. Culpable State of Mind

As already discussed, 2FA never implemented a litigation hold notice at any point in this litigation. At minimum, therefore, Cuttill acted with gross negligence by failing to preserve the computer logs from his late October/early November 2009 investigation. Moreover, Cuttill admitted that he intentionally withheld the logs because of his subjective belief that the logs would have appeared to point falsely to Salyards as the author of the September 3 e-mail. The duty to preserve documents is meant to prevent these sorts of "judgment calls" by litigants and, instead, requires parties to preserve all documents that may reasonably lead to the discovery of relevant

evidence, regardless of whether those documents appear to create false positives or false negatives. See Pension, 2010 WL 184312, at *8 (disparaging document preservation policy that "place[d] total reliance on the employee to search and select what that employee believed to be responsive records"). Thus, 2FA acted in bad faith by failing to preserve records that it thought falsely pointed to Salyards as the author of the September 3 e-mail. The Court holds, therefore, that 2FA's failure to preserve the computer logs from Cuttill's investigation amounts to intentional bad faith spoliation of evidence.

c. Relevance

Because the Court finds that Cuttill intentionally and in bad faith failed to preserve 2FA's computer logs from his investigation, the Court presumes the relevance of these documents, obviating Passlogix's burden to show through extrinsic evidence that these documents would have been favorable to its position. See Pension, 2010 WL 184312, at *5. The burden now shifts to 2FA to demonstrate that Passlogix was not "prejudiced by the absence of the missing information." Id. 2FA states that Passlogix knew about Cuttill's investigation "on December 1st but never requested anything from 2FA . . . and never made any requests in the several appearances before Judge

Dolinger." (Opp'n Mem. 32-33.) This representation clearly misrepresents the record. During a December 22 hearing before Judge Dolinger, which occurred after Cuttill's deposition, Passlogix explicitly requested, and Judge Dolinger ordered 2FA to produce, information from Cuttill's investigation. (See 12/22/09 J. Dolinger Hr'g Tr. 24:24-28:4 (Passlogix's counsel requesting "any notes, findings, documentation surrounding the 2FA internal investigation within the 2FA company concerning the anonymous e-mails" and Judge Dolinger ordering 2FA's counsel to "inquire of [his] client and advise counsel for Passlogix within . . . three days" about 2FA's internal investigation).). There is no dispute that the records that 2FA provided to Passlogix did not include the electronic records from Cuttill's investigation. In defense of its actions, 2FA contends that it agreed to allow Passlogix to conduct forensic examinations on all of 2FA's computers, but Passlogix never did so. (Opp'n Mem. 32-33.) 2FA's argument misses the point. Making its computers available to Passlogix for inspection does not absolve 2FA of its affirmative duty to preserve electronic records that it examined but admittedly failed to preserve. Because 2FA failed to preserve the electronic records, making its computers available for inspection likely would have been a meaningless gesture.

Moreover, 2FA's position that Passlogix never asked for the computer logs—even if true—is disingenuous in light of 2FA preventing Passlogix, on seemingly erroneous privilege grounds, from asking Cuttill during his deposition about the scope of his investigation. (Mem. 4; Tr. 596:22-598:20; 12/22/09 J. Dolinger Hr'g Tr. 24:24-28:4.) 2FA's counsel and Cuttill later admitted that counsel was not involved in Cuttill's investigation. (See Tr. 596:22-597:25; 12/22/09 J. Dolinger Hr'g Tr. 25:10-26:17.) Though considered, the Court declines to issue a separate sanction for 2FA's possibly erroneous assertion of privilege, as the Court deems 2FA's sanction for spoliation of evidence sufficient to prevent future litigation misconduct.

Because Passlogix does not have a copy of 2FA's computer logs and because the logs likely are no longer available as a result of 2FA's continued deletion of records, the Court holds that Passlogix is prejudiced by 2FA's spoliation of these electronic records.

B. Remedy for 2FA's Spoliation of Evidence

"The court has the inherent power to impose sanctions for the spoliation of evidence, even where there has been no explicit order requiring the production of the missing evidence." Scalera, 262 F.R.D. at 171; see also Residential Funding, 306 F.3d at 106-07. "The determination of an

appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis." Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001); see also Reilly v. Natwest Mkts. Group Inc., 181 F.3d 253, 267 (2d Cir. 1999) ("Trial judges should have the leeway to tailor sanctions to insure that spoliators do not benefit from their wrongdoing—a remedial purpose that is best adjusted according to the facts and evidentiary posture of each case."). Sanctions for the spoliation of evidence are meant to (1) deter parties from destroying evidence; (2) place the risk of an erroneous evaluation of the content of the destroyed evidence on the party responsible for its destruction; and (3) restore the party harmed by the loss of evidence helpful to its case to where the party would have been in the absence of spoliation. See Potenza v. Gonzales, Nos. 5:07-CV-225, 5:07-CV-226, 2010 WL 890959, at *3 (N.D.N.Y. Mar. 8, 2010); Byrnie, 243 F.3d at 107; Port Auth. Police Asian Jade Soc'y, 601 F. Supp. 2d at 570. "[A] court should always impose the least harsh sanction that can provide an adequate remedy." Pension, 2010 WL 184312, at *6. "The choices include—from least harsh to most harsh—further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal (terminating sanctions)." Id.

Passlogix asks for three forms of relief for 2FA's spoliation of evidence—an adverse inference, preclusion, and costs. (Mem. 33-34.) The Court declines to impose any of these sanctions, concluding that the most appropriate sanction for 2FA's spoliation of evidence is a monetary fine.

1. Adverse Inference

An adverse inference is warranted where a party intentionally destroys documents that it is obligated to preserve and that are relevant to its adversary's case. See Byrnie, 243 F.3d at 107-08; Kronisch, 150 F.3d at 126. Passlogix asks the Court to infer from the deleted communications between Salyards and Collier that Salyards and Collier conspired to send the anonymous e-mails and to have Collier falsely testify to authoring the April 13 e-mail. In support of its adverse inference request, Passlogix points to phone records and Skype logs indicating that Collier and Salyards communicated during critical points in the litigation: (1) April 13 when the first anonymous e-mail was sent; (2) September 4, 2009, the day after the next anonymous e-mail was sent; and (3) between October 26-28, when Salyards learned that Passlogix was going to, and then did, inform that Court that Salyards authored the anonymous e-mails. (PX 43 Ex. A; PX 45 at CC10 line 212, CC100 line 68, CC124 lines 365-66, 370-71, 383,

CC128 line 191, CC136 line 2; PX 47 at 11690, 11796, 11800, 11857, 11862; PX 50 at PL9618016.) Upon a review of the entire record of communications between Salyards and Collier—including their cell phone records from April through November 2009 and Skype logs from April through October 2009 that Passlogix retrieved from Collier's work computer—Salyards' and Collier's level of communication during critical points in the litigation is consistent with their level of contact throughout the course of the year. Therefore, this extrinsic evidence is inconclusive at best and does not warrant an adverse inference that the two were conspiring to commit a fraud on the court. See Skeete, 1993 WL 256659, at *7 (denying defendant's request for adverse inference "where defendants have not demonstrated a nexus between the content of the materials and the inference the defendants wish to have drawn").

The Court also declines to infer that the 2FA computer network logs that Cuttill failed to preserve would have shown that Salyards authored the September 3 e-mail. Through his testimony at the evidentiary hearing, Cuttill admitted that the 2FA network logs, if preserved, would have indicated that Salyards visited Hush in mid-September. The Court credits this testimony and finds that a further adverse inference is not warranted. See Wechsler v. Hunt Health Sys., Ltd., 381 F. Supp. 2d 135, 148-49 (S.D.N.Y. 2003) (Leisure, J.) (denying request

for a negative inference where, among other things, the absent documents did not have a profound effect on defendant's case).

2. Evidence Preclusion

"Preclusion is a harsh sanction preserved for exceptional cases where a . . . party's failure to provide the requested discovery results in prejudice to the requesting party." Tracey ex rel. v. NVR, Inc., No. 04 Civ. 6541L, 2009 WL 3153150, at *8 n.15 (W.D.N.Y. Sept. 30, 2009) (citation and internal quotation marks omitted); see also Update Art, Inc. v. Modiin Publ'g, Ltd., 843 F.2d 67, 71 (2d Cir. 1988). Passlogix asks that 2FA be precluded from arguing that Collier somehow traced Salyards' whereabouts through Salyards' e-mail headers and somehow spoofed Salyards' IP address as it changed from office, to home, to the Mark Hopkins Hotel. (Mem. 33.) The Court declines Passlogix's preclusion request as too harsh and unwarranted by the evidence in the record, as it would prohibit 2FA from asserting its IP spoofing defense. See Pesce v. Gen. Motors Corp., 939 F. Supp. 160, 165 (N.D.N.Y. 1996) (declining "the drastic sanction of preclusion" where "an order precluding any testimony or evidence of the [product] being defective would necessarily preclude plaintiff from being able to present a prima facie case," "which would be tantamount to dismissal of the action"); see also In re WRT Energy Sec. Litig., 246 F.R.D. 185, 200 (S.D.N.Y. 2007)

(crafting a more narrow remedy where defendants' proposed sanction of precluding plaintiffs from relying on the destroyed documents "in any respect" would "sweep too broadly").

3. Costs

Passlogix requests that 2FA pay for its investigation, which was more costly and protracted as a result of 2FA's spoliation of evidence. (Mem. 34.) "[C]ompensable costs may arise either from the discovery necessary to identify alternative sources of information, or from the investigation and litigation of the document destruction itself." Turner, 142 F.R.D. at 78 (holding that "an award of costs, including attorneys' fees, is entirely warranted" where defendant "unjustifiably destroyed documents after litigation had been commenced, causing the plaintiff to expend time and effort in attempting to track down the relevant information"); see also Pension, 2010 WL 184312, at *24 (sanctioning plaintiffs who were negligent in providing discovery by issuing a monetary sanction of reasonable costs, including attorneys' fees, associated with reviewing declarations submitted, deposing these declarants, and bringing this motion for sanctions).

After careful consideration, the Court holds that costs are not appropriate here where the extra expense incurred by Passlogix—that is related solely to the deletion of electronic

data from Cuttill's investigation and certain communications between Salyards and Collier—cannot be carved out easily from Passlogix's overall costs in litigating the instant dispute. Therefore, a more narrowly tailored sanction that serves to punish 2FA for its grossly negligent failure to institute a litigation hold, intentional failure to preserve electronic records from its investigation, and possibly erroneous assertion of privilege, is more appropriate here.

4. Monetary Fine

The applicable sanction for spoliation of evidence "should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine." West, 167 F.3d at 779; see also In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 93, 148-49 (2d Cir. 2008). Imposing a fine is consistent with the Court's inherent power to sanction parties for the spoliation of evidence. See Pension, 2010 WL 184312, at *6 (considering a fine one of the less harsh remedies a Court may choose from to sanction a party for spoliation of evidence); accord Travelers Property Cas. Of Am. ex rel. Goldman v. Pavillion Dry Cleaners, No. Civ. A. 04-1446, 2005 WL 1366530, at *4 (D.N.J. June 7, 2005) (stating that a monetary fine may be appropriate to punish an offending party for spoliation of evidence).

The Court holds that a monetary fine of $10,000 against 2FA best suits "the facts and evidentiary posture of [this] case." Reilly, 181 F.3d at 267. 2FA is a small company founded only in 2006, and Salyards and Cuttill—who the Court both finds responsible for the spoliation of evidence in this case—are 2FA's sole principals and co-founders. Here, a fine against 2FA serves the dual purposes of deterrence and punishment. See Green, 262 F.R.D. at 292. Because Salyards and Cuttill are the sole principals of 2FA, a fine directed at 2FA will affect them directly. In concluding that a fine of $10,000 is the most appropriate sanction, the Court balances 2FA's litigation conduct with its status as a small corporation. See Shangold v. Walt Disney Co., 275 Fed. Appx. 72, 74 (2d Cir. 2008) (stating that district courts "should not hesitate to take the relative wealth of the parties into account" when setting monetary sanctions, and affirming district court's $10,000 fee award) (citation and internal quotation marks omitted); McMunn, 191 F. Supp. 2d. at 448, 462 (considering defendant's ability to collect from plaintiff in issuing order requiring plaintiff to pay defendant $20,000 with interest for, among other misconduct, "spoil[ing] highly relevant evidence by, intentionally and in bad faith, concealing the existence of [her] Visa Card, [which] . . . was highly prejudicial to [defendant], and . . . never corrected by [plaintiff]"); accord United States v. Philip

Morris USA Inc., 327 F. Supp. 2d 21, 26 (D.D.C. 2004) (holding that a fine of $2,995,000 payable to the Court Registry "is particularly appropriate here because [the Court has] no way of knowing what, if any, value [the] destroyed emails had to Plaintiff's case; [therefore] . . . it [is] impossible to fashion a proportional evidentiary sanction that would accurately target the discovery violation. . . . [Yet], it is essential that such conduct be deterred . . . and that the amount of the monetary sanction fully reflect the reckless disregard and gross indifference displayed by [defendants] toward their discovery and document preservation obligations"); In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 617 (D.N.J. 1997) (imposing $1 million fine, payable to the Clerk of the U.S. District Court for the District of New Jersey, for Prudential's consistent pattern of document destruction, where Prudential violated a court order "on at least four occasions," "ha[d] no comprehensive document retention policy," and "impede[d] the litigation process"; reasoning that the fine "informs Prudential and the public of the gravity of repeated incidents of document destruction and the need of the Court to preserve and protect its jurisdiction and the integrity of the proceedings before it").

CONCLUSION

For the foregoing reasons, the Court holds that neither Passlogix nor 2FA has established by clear and convincing evidence that its adversary committed a fraud on the Court. 2FA's request to amend its counterclaims to assert a cause of action for malicious prosecution against Passlogix is denied on grounds of futility. The Court also holds that 2FA's failure to preserve relevant documents led to the spoliation of evidence in this case. Therefore, the Court hereby orders 2FA to pay a fine in the amount of ten thousand dollars ($10,000.00), via check made payable to "Clerk, U.S. District Court" within thirty (30) days from the date of this Opinion and Order.

SO ORDERED.
New York, New York

April 27, 2010

U.S.D.J.

Copies of this Opinion and Order have been e-mailed to:

Steven M. Kayman, Esq.
Dan Goldberger, Esq.
Proskauer Rose LLP
1585 Broadway
New York, New York 10036-8299

Hal S. Shaftel, Esq.
Cadwalader, Wickersham & Taft LLP
One World Financial Center

New York, N.Y. 10281

Laurence Singer, Esq.
Laurence Singer, Attorney-At-Law
1629 K Street NW, Suite 300
Washington, D.C. 20006